



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  / А.С. Исмагилова

Согласовано:  
Председатель УМК института  
 /Р.А. Гильмутдинова

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Экономическая разведка и контрразведка

Б1.В.1.ДВ.11.02 вариативная


программа бакалавриата

Направление подготовки  
10.03.01 Информационная безопасность

Профиль подготовки  
Организация и технология защиты информации

Квалификация  
бакалавр

Разработчик (составитель)  
к.б.н., доцент

 /Ф.Т. Байрушин

Для приема: 2019 г.

Уфа 2019 г.

Составитель: Ф.Т. Байрушин

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	7
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)	7
4. Фонд оценочных средств по дисциплине	7
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	7
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	13
4.3. Рейтинг-план дисциплины	26
5. Учебно-методическое и информационное обеспечение дисциплины	26
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	26
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины	26
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	27

## 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	Знать основы экономических знаний в различных сферах деятельности	ОК-2 способность использовать основы экономических знаний в различных сферах деятельности	
	Знать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	ОПК-4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	
	Знать 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 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	
	Знать комплекс мер по обеспечению информационной безопасности, управлению процессом их реализации	ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	Знать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	

Умения	Уметь использовать основы экономических знаний в различных сферах деятельности	ОК-2 способность использовать основы экономических знаний в различных сферах деятельности	
	Уметь понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	ОПК-4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	
	Уметь 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 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	
	Уметь принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	Уметь организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	
Владения	Владеть навыками	ОК-2 способность использовать	

(навыки / опыт деятельности)	использования основ экономических знаний в различных сферах деятельности	основы экономических знаний в различных сферах деятельности	
	Владеть понятиями значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации	ОПК-4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	
	Владеть навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	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	
	Владеть навыками принятия участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	Владеть навыками организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и методическими документами Федеральной службы безопасности Российской Федерации	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	

	Федерации, Федеральной службы по техническому и экспортному контролю		
--	--	--	--

## 2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Экономическая разведка и контрразведка» относится к дисциплинам вариативной части профессионального цикла.

Дисциплина изучается на 4 курсе в 8 семестре.

Цель изучения дисциплины: формирование у бакалавров целостного представления об экономической разведке и контрразведке.

## 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

**ОК-2** способность использовать основы экономических знаний в различных сферах деятельности

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать основы экономических знаний в различных сферах деятельности	Не знает или имеет фрагментарные знания об основах экономических знаний в различных сферах деятельности	В целом знает основы экономических знаний в различных сферах деятельности
Второй этап (уровень)	Уметь использовать основы экономических знаний в различных сферах деятельности	Не умеет или не способен использовать основы экономических знаний в различных сферах деятельности	Умеет систематически использовать основы экономических знаний в различных сферах деятельности

Третий этап (уровень)	Владеть методами использования основ экономических знаний в различных сферах деятельности	Не владеет методами использования основ экономических знаний в различных сферах деятельности	Способен систематически использовать основы экономических знаний в различных сферах деятельности
-----------------------	---	--	--

**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	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать значение информации в развитии современного общества, информационные технологии для поиска и обработки информации	Не знает или имеет фрагментарные знания о значении информации в развитии современного общества, о применении информационных технологий для поиска и обработки информации	В целом знает основы значение информации в развитии современного общества, применения информационных технологий для поиска и обработки информации
Второй этап (уровень)	Уметь понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Не умеет или не способен понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Умеет систематически понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
Третий этап (уровень)	Владеть понятиями значения информации в развитии современного общества, применения информационных те	Не владеет понятиями значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации	Способен систематически понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации



	хнологий для поиска и обработки 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	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать 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	Не знает или имеет фрагментарные знания об информационных ресурсах, подлежащих защите, угрозах безопасности информации и возможных путях их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	В целом знает 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
Второй этап (уровень)	Уметь 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	Не умеет или не способен 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	Умеет систематически 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

Третий этап (уровень)	Владеть навыками 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	Не владеет навыками 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	Способен систематически применять навыки 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

**ПК-13** способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать комплекс мер по обеспечению информационной безопасности, управлению процессом их реализации	Не знает или имеет фрагментарные знания о комплексе мер по обеспечению информационной безопасности, управлению процессом их реализации	В целом знает комплекс мер по обеспечению информационной безопасности, управлению процессом их реализации
Второй этап (уровень)	Уметь принимать участие в формировании, организовывать и поддерживать выполнение	Не умеет или не способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по	Умеет систематически принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по

	комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	обеспечению информационной безопасности, управлять процессом их реализации	обеспечению информационной безопасности, управлять процессом их реализации
Третий этап (уровень)	Владеть навыками принятия участия в формировании, организации и поддержке выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации	Не владеет навыками принятия участия в формировании, организации и поддержке выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации	Способен систематически применять навыки принятия участия в формировании, организации и поддержке выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации

**ПК-15** способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать организацию технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации	Не знает или имеет фрагментарные знания об организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации	В целом знает комплекс мер по организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

	Федерации, Федеральной службы по техническому и экспортному контролю	и экспортному контролю	
Второй этап (уровень)	Уметь организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Не умеет или не способен организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Умеет систематически организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
Третий этап (уровень)	Владеть навыками организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Не владеет навыками организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Способен систематически использовать навыки организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

	техническому и экспортному контролю		
--	-------------------------------------	--	--

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

Шкала оценивания для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),  
не зачтено – от 0 до 59 рейтинговых баллов).

**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**

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	Знать основы экономических знаний в различных сферах деятельности	ОК-2 способность использовать основы экономических знаний в различных сферах деятельности	Опрос, практические задания, тестирование
	Знать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	ОПК-4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Опрос, практические задания, тестирование
	Знать 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 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	Опрос, практические задания, тестирование, лабораторная работа

	Знать комплекс мер по обеспечению информационной безопасности, управлению процессом их реализации	ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Опрос, практические задания, тестирование, лабораторная работа
	Знать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Опрос, практические задания, тестирование лабораторная работа,
2-й этап Умения	Уметь использовать основы экономических знаний в различных сферах деятельности	ОК-2 способность использовать основы экономических знаний в различных сферах деятельности	Опрос, практические задания, тестирование, лабораторная работа
	Уметь понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	ОПК-4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Опрос, практические задания, тестирование
	Уметь определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и	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	Опрос, практические задания, тестирование

	особенностей функционирования объекта защиты	функционирования объекта защиты	
	Уметь принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Опрос, практические задания, тестирование, лабораторная работа
	Уметь организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Опрос, практические задания, тестирование, лабораторная работа
3-й этап Владения навыками	Владеть навыками использования основ экономических знаний в различных сферах деятельности	ОК-2 способность использовать основы экономических знаний в различных сферах деятельности	Опрос, практические задания, тестирование
	Владеть понятиями значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации	ОПК-4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Опрос, практические задания, тестирование, лабораторная работа
	Владеть навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе	ОПК-7 способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры	Опрос, практические задания, тестирование, лабораторная работа

	анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	и содержания информационных процессов и особенностей функционирования объекта защиты	
	Владеть навыками принятия участия в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Опрос, практические задания, тестирование лабораторная работа
	Владеть навыками организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Опрос, практические задания, тестирование лабораторная работа

### **Устный индивидуальный опрос**

Устный индивидуальный опрос проводится на семинарских занятиях в рамках изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации.

#### **Примерная тематика семинарских занятий**

##### **Модуль №1**

- 1) Международная экономическая безопасность и особенности обеспечения национальной экономической безопасности России.
- 2) Понятие национальной экономической безопасности.
- 3) Особенности обеспечения национальной экономической безопасности России.

##### **Модуль №2**

- 1) Проблемы НЭБ, связанные с либерализацией экономики.



- 2) Понятие экономической безопасности предприятия и его элементы.
- 3) Механизм обеспечения экономической безопасности предприятия.

Студент излагает содержание вопроса изученной темы, в соответствии с тематикой практических занятий.

Критерии и методика оценивания:

- 3 балла выставляется студенту, если точно используется специализированная терминология, показано уверенное владение нормативной базой;
- 2 балла выставляется студенту, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология, имеются определенные затруднения;
- 1 балл выставляется студенту, если в логическом рассуждении есть существенные ошибки; не совсем правильно сделан выбор формулировок, нет определенной логической последовательности, неточно используется специализированная терминология;
- 0 балла выставляется студенту, если допущены грубые ошибки в определении понятий, использовании терминологии или студент не готов к ответу.

### **Типовые задания для практических работ**

#### **Модуль 1**

- 1) Международная экономическая безопасность и особенности обеспечения национальной экономической безопасности России.
- 2) Разведка и контрразведка как органы безопасности: история, терминология, актуальность, правовые основы.
- 3) Понятие, виды и основные объекты разведывательной и контрразведывательной деятельности.
- 4) Сыск, разведка, контрразведка и частная детективная деятельность.

#### **Модуль 2**

- 5) Методы научного познания на службе в контрразведке.
- 6) Государство и контрразведка.
- 7) Разведка, контрразведка и бизнес.
- 8) Внешние угрозы безопасности негосударственных хозяйствующих субъектов.

Критерии и методика оценивания:

- 2,5 балла выставляется студенту, если составлен верный ответ, показано уверенное владение нормативной базой;
- 1 балл выставляется студенту, если в логическом рассуждении нет существенных ошибок; правильно сделан выбор формулировок, но допущено не более двух несущественных ошибок, получен верный ответ, нет определенной логической последовательности, неточно используется специализированная терминология;
- 0 баллов выставляется студенту, если студент не дал ни одного правильного ответа

### **Типовые задания для лабораторных работ**

1. Система безопасности негосударственных хозяйствующих субъектов в России
2. Информационно-аналитическая работа в системе экономической разведки и контрразведки

Критерии и методика оценивания:

- 6 баллов выставляется студенту, если составлен верный ответ, показано уверенное владение нормативной базой;

- 5 балл выставляется студенту, если в логическом рассуждении нет существенных ошибок; правильно сделан выбор формулировок, но допущено не более двух несущественных ошибок, получен верный ответ;

4 балла выставляется студенту, если в логическом рассуждении есть существенные ошибки; не совсем правильно сделан выбор формулировок,

3 балла выставляется студенту, если в логическом рассуждении есть существенные ошибки, неточно используется специализированная терминология

2 балла выставляется студенту, если нет определенной логической последовательности, неточно используется специализированная терминология

1 балл выставляется студенту, если нет определенной логической последовательности, неточно используется специализированная терминология

- 0 баллов выставляется студенту, если студент не дал ни одного правильного ответа

### Тестирование

Вопрос 1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...

- 1) политическая разведка;
- 2) промышленный шпионаж;
- 3) добросовестная конкуренция;
- 4) конфиденциальная информация;
- 5) правильного ответа нет.

Вопрос 2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности ?

- 1) любая информация;
- 2) только открытая информация;
- 3) запатентованная информация;
- 4) закрываемая собственником информация;
- 5) коммерческая тайна.

Вопрос 3. Кто может быть владельцем защищаемой информации?

- 1) только государство и его структуры;
- 2) предприятия акционерные общества, фирмы;
- 3) общественные организации;
- 4) только вышеперечисленные;
- 5) кто угодно.

Вопрос 4. Какие сведения на территории РФ могут составлять коммерческую тайну?

- 1) учредительные документы и устав предприятия;
- 2) сведения о численности работающих, их заработной плате и условиях труда;
- 3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
- 4) другие;
- 5) любые.

Вопрос 5. Какие секретные сведения входят в понятие «коммерческая тайна»?

- 1) связанные с производством;
- 2) связанные с планированием производства и сбытом продукции;
- 3) технические и технологические решения предприятия;
- 4) только 1 и 2 вариант ответа;
- 5) три первых варианта ответа.

Вопрос 5. Что называют источником конфиденциальной информации?

- 1) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников;
- 2) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе;
- 3) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники;
- 4) это защищаемые предприятием сведения в области производства и коммерческой деятельности;
- 5) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.

Вопрос 6. Как называют процессы обмена информацией с помощью официальных, деловых документов?

- 1) непосредственные;
- 2) межличностные;
- 3) формальные;
- 4) неформальные;
- 5) конфиденциальные.

Вопрос 7. Какое наиболее распространенное действие владельца конфиденциальной информации, приводит к неправомерному овладению ею при минимальных усилиях со стороны злоумышленника?

- 1) хищение носителей информации;
- 2) использование технических средств для перехвата электромагнитных ПЭВМ;
- 3) разглашение;
- 4) копирование программой информации с носителей;
- 5) другое.

Вопрос 8. Каким образом происходит разглашение конфиденциальной информации?

- 1) утеря документов и других материалов, или пересылка их посредством почты, посыльного, курьера;
- 2) опубликование материалов в печати;
- 3) сообщение, передача, предоставление в ходе информационного обмена;
- 4) все вышеперечисленные способы;
- 5) правильного варианта ответа нет.

Вопрос 9. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

- 1) получить, изменить, а затем передать ее конкурентам;
- 2) размножить или уничтожить ее;
- 3) получить, изменить или уничтожить;
- 4) изменить и уничтожить ее;
- 5) изменить, повредить или ее уничтожить.

Вопрос 10. Какой самый прямой и эффективный способ склонения к сотрудничеству?

- 1) психическое давление;
- 2) подкуп;
- 3) преследование;
- 4) шантаж;
- 5) угрозы.

Вопрос 11. Наиболее сложный и дорогостоящий процесс несанкционированного доступа к источникам конфиденциальной информации?

- 1) инициативное сотрудничество;
- 2) выпытывание;
- 3) наблюдение;
- 4) хищение;

5) копирование.

Вопрос 12. Какое из утверждений неверно?

- 1) подкуп — сложный процесс, требует долгой и кропотливой работы;
- 2) выпытывание — это стремление путем внешне наивных вопросов получить определенные сведения;
- 3) процесс наблюдения не сложен, так как не требует затрат сил и средств;
- 4) под незаконным подключением понимают контактное или бесконтактное подсоединение к линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них;
- 5) негласное ознакомление — способ получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность кое-что узнать.

Вопрос 13. Завершающим этапом любого сбора конфиденциальной информации является

- 1) копирование;
- 2) подделка;
- 3) аналитическая обработка;
- 4) фотографирование;
- 5) наблюдение.

Вопрос 14. Как называются реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации?

- 1) ненадежность;
- 2) угроза;
- 3) несчастный случай;
- 4) авария;
- 5) правильного ответа среди перечисленных нет.

Вопрос 15. Что в скором времени будет являться главной причиной информационных потерь?

- 1) материальный ущерб, связанный с несчастными случаями;
- 2) кража и преднамеренная порча материальных средств;
- 3) информационные инфекции;
- 4) аварии и выход из строя аппаратуры, программ и баз данных;
- 5) ошибки эксплуатации.

Вопрос 16. В каком варианте ответа инфекции расположены от более простого к более сложному, по возрастанию?

- 1) логические бомбы, троянский конь, червь, вирус;
- 2) червь, вирус логические бомбы, троянский конь;
- 3) червь логические бомбы вирус, троянский конь;
- 4) логические бомбы, вирус, троянский конь червь;
- 5) вирус, логические бомбы, троянский конь червь.

Вопрос 17. Причины связанные с информационным обменом приносящие наибольшие убытки?

- 1) остановка или выход из строя информационных систем;
- 2) потери информации;
- 3) неискренность;
- 4) проникновение в информационную систему;
- 5) перехват информации.

Вопрос 18. Какие цели преследуются при активном вторжении в линии связи?

- 1) анализ информации(содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;
- 2) воздействие на поток сообщений(модификация, удаление и посылка ложных сообщений) или восприпятствие передаче сообщений;

- 3) инициализация ложных соединений;
- 4) варианты 1 и 2;
- 5) варианты 2 и 3.

Вопрос 19. Что определяет модель нарушителя?

- 1) категории лиц, в числе которых может оказаться нарушитель;
- 2) возможные цели нарушителя и их градации по степени важности и опасности;
- 3) предположения о его квалификации и оценка его технической вооруженности;
- 4) ограничения и предположения о характере его действий;
- 5) все выше перечисленные.

Вопрос 20. Выберите наиболее полный список мотивов, которые преследуют компьютерные пираты (хакеры), пытаясь получить несанкционированный доступ к информационной системе или вычислительной сети.

- 1) ознакомление с информационной системой или вычислительной сетью;
- 2) похитить программу или иную информацию;
- 3) оставить записку, выполнить, уничтожить или изменить программу;
- 4) вариант 2 и 3;
- 5) вариант 1, 2 и 3.

Вопрос 21. Какое из утверждений неверно?

- 1) наблюдается тенденция к стремительному росту попыток получить несанкционированный доступ к информационным системам или вычислительным сетям;
- 2) недовольный руководителем служащий создает одну из самых больших угроз вычислительным системам коллективного пользования;
- 3) считается, что компьютерные преступления, более легкий путь добывания денег, чем ограбление банков;
- 4) очень малое число фирм могут пострадать от хакеров;
- 5) к категории хакеров-профессионалов обычно относят: преступные группировки, преследующие политические цели.

Вопрос 22. Какое из утверждений неверно?

- 1) хакеры могут почерпнуть много полезной информации из газет и других периодических изданий;
- 2) хакерами часто используется завязывание знакомств для получения информации о вычислительной системе или выявления служебных паролей;
- 3) один из наиболее эффективных и наименее рискованных путей получения конфиденциальной информации и доступа к ЭВМ — просто изучая черновые распечатки;
- 4) перехват сообщений в каналах связи может идти лишь в связи с деятельностью военных или секретных служб;
- 5) после получения необходимого объема предварительной информации, компьютерный хакер-профессионал осуществляет непосредственное вторжение в систему.

Вопрос 23. Какое из утверждений неверно?

- 1) наибольшие убытки (в среднем) приносит саботаж в нематериальной сфере;
- 2) убытки, связанные с забастовками не превышают убытков связанных с аварией оборудования;
- 3) уход ведущих специалистов опасен для малых центров;
- 4) хищения, в первую очередь осуществляются сотрудниками предприятия или пользователями;
- 5) аварии оборудования или основных элементов системы являются мало распространенными и определяются надежностью аппаратуры.

Вопрос 24. Метод скрытие — это...

- 1) максимальное ограничение числа секретов, из-за допускаемых к ним лиц;
- 2) максимального ограничения числа лиц, допускаемых к секретам;

- 3) уменьшение числа секретов неизвестных большинству сотрудников;
- 4) выбор правильного места, для утаивания секретов от конкурентов;
- 5) поиск максимального числа лиц, допущенных к секретам.

Вопрос 25. Что включает в себя ранжирование как метод защиты информации?

- 1) регламентацию допуска и разграничение доступа к защищаемой информации;
- 2) деление засекречиваемой информации по степени секретности;
- 3) наделять полномочиями назначать вышестоящими нижестоящих на соответствующие посты;
- 4) вариант ответа 1 и 2;
- 5) вариант ответа 1, 2 и 3.

## **Модуль 2**

Вопрос 1. К какому методу относятся следующие действия: имитация или искажение признаков и свойств отдельных элементов объектов защиты, создания ложных объектов?

- 1) скрытие;
- 2) дезинформация;
- 3) дробление;
- 4) кодирование;
- 5) шифрование.

Вопрос 2. Что в себя морально-нравственные методы защиты информации?

- 1) воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений;
- 2) контроль работы сотрудников, допущенных к работе с секретной информацией;
- 3) обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;
- 4) вариант ответа 1 и 3;
- 5) вариант ответа 1, 2 и 3.

Вопрос 3. Какое из выражений неверно?

- 1) страхование — как метод защиты информации пока еще не получил признания;
- 2) кодирование — это метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации;
- 3) шифрование может быть предварительное и линейное;
- 4) дирекция очень часто не может понять необходимость финансирования безопасности;
- 5) безопасность предприятия — не стабильное состояние предприятия, не поддающееся прогнозированию во времени.

Вопрос 4. Какой должна быть защита информации с позиции системного подхода?

- 1) безопасной для сотрудников;
- 2) активной;
- 3) универсальной;
- 4) надежной;
- 5) непрерывной.

Вопрос 5. Что такое «служба безопасности»?

- 1) система внештатных формирований, предназначенных для обеспечения безопасности объекта;
- 2) структурное подразделение, предназначенное для охраны помещений и территорий предприятия;
- 3) система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности и защиты конфиденциальной информации;
- 4) структурное подразделение, предназначенное для хранения и выдачи документов, носителей конфиденциальной информации;
- 5) структурное подразделение, задача которого: подбор персонала и работа с сотрудниками.

Вопрос 6. Кому подчиняется служба безопасности?

- 1) владельцу предприятия;
- 2) владельцу предприятия и лицу которому тот подчиняется;
- 3) руководителю предприятия, либо лицу, которому тот делегировал свои права по руководству ее деятельностью;
- 4) заместителю руководителя предприятия по организационным вопросам;
- 5) только начальнику службы безопасности.

Вопрос 7. Какие задачи не входят в круг обязанностей службы безопасности ?

- 1) внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической безопасности предприятия;
- 2) определение участков сосредоточения сведений, составляющих коммерческую тайну;
- 3) определение на предприятии технологического оборудования, выход из строя которого может привести к большим экономическим потерям;
- 4) ограничение круга сторонних предприятий, работающих с данным предприятием, на которых возможен выход из-под контроля сведений составляющих коммерческую тайну предприятия;
- 5) определение круга сведений, составляющих коммерческую тайну.

Вопрос 8. Какие средства использует инженерно-техническая защита (по функциональному назначению)?

- 1) программные, аппаратные, криптографические, технические;
- 2) программные, физические, шифровальные, криптографические;
- 3) программные, аппаратные, криптографические физические;
- 4) физические, аппаратные, материальные, криптографические;
- 5) аппаратные, физические, программные, материальные.

Вопрос 9. В каком нормативном акте говорится о формировании и защите информационных ресурсов как национального достояния?

- 1) в Конституции РФ;
- 2) в Законе об оперативно розыскной деятельности;
- 3) в Законе об частной охране и детективной деятельности;
- 4) в Законе об информации, информатизации и защите информации;
- 5) в Указе Президента РФ № 170 от 20 января 1994 г. «Об основах государственной политики в сфере информатизации».

Вопрос 10. На какую структуру возложены организационные, коммерческие и технические вопросы использования информационных ресурсов страны

- 1) Министерство Информатики РФ;
- 2) Комитет по Использованию Информации при Госдуме;
- 3) Росинформресурс;
- 4) все выше перечисленные;
- 5) правильного ответа нет.

Вопрос 11. На каком уровне защиты информации создаются комплексные системы защиты информации?

- 1) на организационно-правовом;
- 2) на социально политическом;
- 3) на тактическом;
- 4) на инженерно-техническом;
- 5) на всех вышеперечисленных.

Вопрос 12. Какие существуют наиболее общие задачи защиты информации на предприятии?

- 1) снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной;
- 2) предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;

- 3) документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы;
- 4) создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия;
- 5) все вышеперечисленные.

Вопрос 13. Какие меры и методы защиты секретной или конфиденциальной информации в памяти людей не являются основными?

- 1) воспитание понимания важности сохранения в тайне доверенных им секретных или конфиденциальных сведений;
- 2) подбор людей, допускаемых к секретным работам;
- 3) обучение лиц, допущенных к секретам, правилам их сохранения;
- 4) добровольное согласие на запрет работы по совместительству у конкурентов;
- 5) стимулирование заинтересованности работы с засекреченной информацией и сохранения этих сведений в тайне.

Вопрос 14. В каком документе содержатся основные требования к безопасности информационных систем в США?

- 1) в красной книге;
- 2) в желтой прессе;
- 3) в оранжевой книге;
- 4) в черном списке;
- 5) в красном блокноте.

Вопрос 15. Какое определение соответствует термину «Аутентификация»?

- 1) набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации в данной организации;
- 2) распознавание имени объекта;
- 3) подтверждение того, что предъявленное имя соответствует объекту;
- 4) регистрация событий, позволяющая восстановить и доказать факт происшествия событий;
- 5) правильного определения нет.

Вопрос 16. Какое требование относится к термину «Подотчетность»?

- 1) субъекты индивидуально должны быть идентифицированы;
- 2) гарантированно защищенные механизмы, реализующие указанные базовые требования, должны быть постоянно защищены от "взломывания";
- 3) необходимо иметь явную и хорошо определенную политику обеспечения безопасности;
- 4) аудиторская информация должна храниться и защищаться так, чтобы имелась возможность отслеживать действия, влияющие на безопасность;
- 5) метки, управляющие доступом, должны быть установлены и связаны с объектами.

Вопрос 17. Какой уровень безопасности системы соответствует низшему?

- 1) А;
- 2) В;
- 3) С;
- 4) D;
- 5) E.

Вопрос 18. Какой класс присваивается системам которые не прошли испытания?

- 1) A1;
- 2) B2;
- 3) B3;
- 4) C4;
- 5) D.

Задание 19

Вопрос 1. Что включают в себя технические мероприятия по защите информации?



- 1) поиск и уничтожение технических средств разведки;
- 2) кодирование информации или передаваемого сигнала;
- 3) подавление технических средств постановкой помехи;
- 4) применение детекторов лжи;
- 5) все вышеперечисленное.

Вопрос 20. Какие устройства поиска технических средств разведки не относятся к устройствам поиска пассивного типа?

- 1) металлоискатели;
- 2) тепловизоры;
- 3) устройства и системы поиска по электромагнитному излучению;
- 4) акустические корреляторы;
- 5) детекторы записывающей аппаратуры.

Вопрос 21. Какие устройства не относятся к устройствам поиска по электромагнитному излучению?

- 1) частотомер;
- 2) шумомер;
- 3) сканер;
- 4) нелинейный локатор;
- 5) анализатор спектра.

Вопрос 22. Какова цена самого дешевого японского компактного приемника-сканера?

- 1) 200 US\$.
- 2) 300 US\$.
- 3) 500 US\$.
- 4) 700 US\$.
- 5) 900 US\$.

Вопрос 23. Какова дальность обнаружения звукозаписывающей аппаратуры?

- 1) 1 м.
- 2) более 1 м.
- 3) менее 1 м.
- 4) 3 м.
- 5) 5 м.

Вопрос 24. Какова скорость перемешивания частотных интервалов при частотном скремблировании?

- 1) 1 цикл в сек.
- 2) 20 циклов в сек.
- 3) От 20 до 30 циклов в сек.
- 4) От 2 до 16 циклов в сек.
- 5) От 30 до 40 циклов в сек.

Вопрос 25. С какого расстояния можно считать информацию с монитора компьютера?

- 1) 200 м.
- 2) менее 200 м.
- 3) 500 м.
- 4) 750 м.
- 5) 1 км.

Критерии оценки тестовых заданий в 1 и 2 модуле ОФО

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	0/1 за один ответ Всего: 25 баллов

## Типовые материалы к зачету

- 1) Международная экономическая безопасность и особенности обеспечения национальной экономической безопасности России.
- 2) Понятие национальной экономической безопасности.
- 3) Особенности обеспечения национальной экономической безопасности России.
- 4) Проблемы НЭБ, связанные с либерализацией экономики.
- 5) Понятие экономической безопасности предприятия и его элементы.
- 6) Механизм обеспечения экономической безопасности предприятия.
- 7) Разведка и контрразведка как органы безопасности: история, терминология, актуальность, правовые основы.
- 8) Понятие, виды и основные объекты разведывательной и контрразведывательной деятельности.
- 9) Сыск, разведка, контрразведка и частная детективная деятельность.
- 10) Методы научного познания на службе в контрразведке.
- 11) Государство и контрразведка.
- 12) Разведка, контрразведка и бизнес.
- 13) Внешние угрозы безопасности негосударственных хозяйствующих субъектов.
- 14) Система безопасности негосударственных хозяйствующих субъектов в России.
- 15) Контрразведывательная работа в процессе приема на работу сотрудников негосударственных хозяйствующих субъектов.
- 16) Контрразведывательное обеспечение переговоров.
- 17) Персонал негосударственных хозяйствующих субъектов как объект внимания контрразведки.
- 18) Организационное и кадровое обеспечение подразделения контрразведки.
- 19) Агентура – главное оружие разведки и контрразведки.
- 20) Контрразведывательные мероприятия.
- 21) Контрразведывательный процесс

Критерии оценки (в баллах):

- «Зачтено» выставляется студенту, если он набрал по результатам изучения дисциплины 60 баллов;

- «Не зачтено» выставляется студенту, если он набрал менее 59 баллов.

### 4.3. Рейтинг-план дисциплины (при необходимости)

Рейтинг–план дисциплины представлен в приложении 2.

## 5. Учебно-методическое и информационное обеспечение дисциплины

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

#### Основная литература

1 Лукаш Ю.А. Бизнес-разведка как составляющая обеспечения безопасности и развития бизнеса: учебное пособие: учебное пособие [Электронный ресурс] - Москва: Издательство «Флинта», 2017 137 с. ISBN: 978-5-9765-1378-5-Режим доступа [http://biblioclub.ru/index.php?page=book\\_red&id=114954](http://biblioclub.ru/index.php?page=book_red&id=114954)

2 Стоюхина Н.Ю. История советской психотехники : психология воздействия: учебное пособие[Электронный ресурс]/Н.Ю. Стоюхина.- М.: Логос, 2014.-323с. ISBN: 978-5-98704-679-1 Режим доступа [http:// http://biblioclub.ru/index.php?page=book\\_red&id=119473&sr=1](http://biblioclub.ru/index.php?page=book_red&id=119473&sr=1)

### Дополнительная литература

1. Антонов В.С. Служба внешней разведки : история, люди, факты: Научно-популярная литература [Электронный ресурс]/.- Москва: Кучково поле, 2014 .-384с. ISBN: : 978-5-9950-0339-7 Режим доступа [http://biblioclub.ru/index.php?page=book\\_red&id=454410](http://biblioclub.ru/index.php?page=book_red&id=454410)
- 2.. Козлова В.А. Психология манипулирования: учебно-методическое пособие[Электронный ресурс]/ В.А. Козлова.- Орел: МАБИВ, 2014.-93с Режим доступа [http:// biblioclub.ru/index.php?page=book\\_red&id=428608&sr=1](http://biblioclub.ru/index.php?page=book_red&id=428608&sr=1)

### 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/catalogi/>
5. [www.fstec.ru](http://www.fstec.ru) –сайт ФСТЭК России
6. [www.fsb.ru](http://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/> – 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](http://www.newlibrary.ru) – Новая электронная библиотека;
10. [www.edu.ru](http://www.edu.ru) – Федеральный портал российского образования;
11. [www.elibrary.ru](http://www.elibrary.ru) – Научная электронная библиотека;
12. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
13. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
14. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
<b>1. учебная аудитория для проведения занятий лекционного типа:</b> аудитория № 403 (гуманитарный корпус),	Лекции, практические занятия, лабораторные занятия,	<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.	1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows

<p>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), Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507 (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><b>4. учебная аудитория для проведения групповых и индивидуальных консультаций:</b> аудитория № 403 (гуманитарный корпус), аудитория № 415</p>	<p>групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация</p>	<p><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><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><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><b>Аудитория № 416</b> Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p><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><b>Аудитория № 419</b> Учебная мебель, Проектор Optoma Ex542 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, 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</p>	<p>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 централизованно о тестирования БашГУ (Moodle).GNU General Public License..</p>
--	--	--	---

<p>(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).  <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).  <b>6. помещения для самостоятельной работы:</b> читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).  <b>7.помещение для хранения и профилактического обслуживания учебного оборудования:</b> аудитория № 523 (гуманитарный корпус).</p>		<p>Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром.  <b>Аудитория № 516</b>  Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.  <b>Аудитория № 509</b>  Учебная мебель, доска, мобильное мультимедийное оборудование.  <b>Аудитория № 510</b>  Учебная мебель, доска, мобильное мультимедийное оборудование.  <b>Аудитория № 608</b>  Учебная мебель, доска, мобильное мультимедийное оборудование.  <b>Аудитория № 609</b>  Учебная мебель, доска, мобильное мультимедийное оборудование.  <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.  <b>Аудитория № 613</b>  Учебная мебель, доска, моноблок стационарный – 15 шт.  <b>Компьютерный класс аудитория № 420</b>  Учебная мебель, моноблоки стационарные 15 шт.  <b>Компьютерный класс аудитория № 404</b>  Учебная мебель, компьютеры -15 штук.  <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.  <b>Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507</b>  Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК".  <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 "Зодиак II", универсальный ком-плект инструментов для проведения работ по специальным провер-кам и специальным</p>	
---	--	---	--

		обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031М "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон". <b>Аудитория № 523</b> Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	
--	--	--	--

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ  
дисциплины «Экономическая разведка и контрразведка»  
на 8 семестр

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	36,2
лекций	18
практических / семинарских	10
лабораторных работ	8
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) ФКР	0,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к зачету	35,8

Форма контроля  
Зачет 8 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	3	4	5	6	7	8	9
1	Понятие, виды и основные объекты разведывательной и контрразведывательной деятельности	2			4	Основная 1, 2 Дополнительная 1,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, лабораторные работы, тестирование
2	Государство и контрразведка	2	2		4	Основная 1, 2 Дополнительная 1,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, лабораторные работы, тестирование
3	Сыск, разведка, контрразведка и частная детективная деятельность	2	2		4	Основная 1, 2 Дополнительная 1,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-	Опрос, практические задания, лабораторные работы, тестирование



							источников.	
4	Система безопасности негосударственных хозяйствующих субъектов в России	2		4	4	Основная 1, 2 Дополнительная 1,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, лабораторные работы, тестирование
5	Контрразведывательная работа в процессе приема на работу сотрудников негосударственных хозяйствующих субъектов.	2	2		4	Основная 1, 2 Дополнительная 1,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, лабораторные работы, тестирование
6	Информационно-аналитическая работа в системе экономической разведки и контрразведки	2		4	4	Основная 1, 2 Дополнительная 1,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, лабораторные работы, тестирование
7	Деятельность разведки и контрразведки по выявлению и предупреждению диверсий	4	2		6	Основная 1, 2 Дополнительная 1,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, лабораторные работы, тестирование

8	Деятельность разведки и контрразведки по выявлению и предупреждению мошенничества	2	2		5,8	Основная 1, 2 Дополнительная 1,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Опрос, практические задания, лабораторные работы, тестирование
	Всего	18	10	8	35,8			

Приложение 2

**Рейтинг – план дисциплины**  
**Экономическая разведка и контрразведка**

Курс 4, семестр 8 г

Направление подготовки 10.03.01 «Информационная безопасность»

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
<b>Модуль 1</b>				
Текущий контроль			0	25
1. Аудиторная работа	3	3	0	9
2. Лабораторные работы	6	1	0	6
3. Практические работы	2,5	4	0	10
Рубежный контроль				25
1. Тестовые задания	1	25	0	25
Всего			0	50
<b>Модуль 2</b>				
Текущий контроль			0	25
1. Аудиторная работа	3	3	0	9
2. Лабораторные работы	6	1	0	6
3. Практические работы	2,5	4	0	10
Рубежный контроль				25
1. Тестовые задания	1	25	0	25
Всего			0	50
<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>				
зачет			0	