



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

Актуализировано:  
на заседании кафедры  
протокол от «07» июня 2018 г. № 10  
Зав. кафедрой  /А.С. Исмагилова

Согласовано:  
Председатель УМК института  
 /Р.А. Гильмутдинова

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Системы защиты информации в ведущих зарубежных странах  
Б1.Б.30 базовая

программа бакалавриата

Направление подготовки  
10.03.01 Информационная безопасность

Профиль подготовки  
Организация и технология защиты информации

Квалификация  
бакалавр

Разработчик (составитель)  
к.ф.-м.н., доцент



/И.А. Шагапов

Для приема: 2015 г.

Уфа 2018 г.

Составитель: доцент И.А. Шагапов

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью  
Протокол № 10 от «07» июня 2018 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 .....  | 6  |
| 3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся).....  | 6  |
| 4. Фонд оценочных средств по дисциплине .....   | 6  |
| 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 .....   | 6  |
| 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..... | 19 |
| 4.3. Рейтинг-план дисциплины.....   | 21 |
| 5. Учебно-методическое и информационное обеспечение дисциплины .....  | 28 |
| 5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины .....   | 28 |
| 5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины .....   | 29 |
| 6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине .....  | 29 |

## 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 (модулю):

| Результаты обучения |  | Формируемая компетенция (с указанием кода)  | Примечание |
|---------------------|--|---|------------|
| Знания              | 1. Знать основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, процесс становления систем защиты информации в ведущих зарубежных странах, особенности государственной политики в области защиты информации, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности | ОК-4. Способность использовать основы правовых знаний в различных сферах деятельности   |            |
|                     | 2. Знать нормативные документы для обоснования безопасности конфиденциальной информации в информационных системах, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, достижения международного опыта организации и совершенствования систем защиты информации   | ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности |            |
|                     | 3. Знать технологии обеспечения защиты и сохранности конфиденциальных документов, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, правовые и организационные основы защиты информации в ведущих зарубежных странах тенденции и перспективы развития международного сотрудничества в данной области                             | ПСК-1. Способность участвовать в разработке подсистемы управления информационной безопасностью  |            |
|                     | 1. Знать состояние законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития  | ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью   |            |

|                                       |   |   |  |
|---------------------------------------|---|---|--|
|                                       | систем защиты информации в ведущих зарубежных странах   |   |  |
| Умения                                | 1. Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности  | ОК-4. Способность использовать основы правовых знаний в различных сферах деятельности   |  |
|                                       | 2. Уметь собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности  | ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности |  |
|                                       | 3. Уметь конфигурировать и использовать средства защиты информации в ОС и прикладных программах, настраивать антивирусные программы и другие средства борьбы с программными закладками, применять технические средства защиты данных, проводить анализ защищенности объектов и определять класс защиты информации по международным стандартам.  | ПСК-1. Способность участвовать в разработке подсистемы управления информационной безопасностью  |  |
|                                       | 4. Уметь обосновывать организационно-технические мероприятия по защите информации.  | ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью   |  |
| Владения (навыки / опыт деятельности) | 1. Владеть навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности  | ОК-4. Способность использовать основы правовых знаний в различных сферах деятельности   |  |
|                                       | 2. Владеть навыками сбора и обработки необходимых данных; навыками анализа и интерпретации содержащейся в различных источниках информации, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, иметь представление о международных стандартах безопасности, включая стратегии их мониторинга и аудита, определения | ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности |  |

|  |  |   |  |
|--|--|---|--|
|  | целей, уровней безопасности и их важности.   |   |  |
|  | 3. Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий  | ПСК-1. Способность участвовать в разработке подсистемы управления информационной безопасностью                    |  |
|  | 4. Владеть навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности; эксплуатации современного электронного оборудования и информационно-коммуникационных технологий | ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью |  |

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

Дисциплина «Системы защиты информации в ведущих зарубежных странах» относится к обязательным дисциплинам базовой части.

Дисциплина изучается на 3,4 курсах в 6,7 семестрах.

Целью освоения дисциплины является раскрытие фундаментальных представлений гуманитарных наук об организационно-правовом обеспечении деятельности государственных и частных структур развитых зарубежных стран по защите информации, что дает возможность сравнить отечественный и зарубежный опыт обеспечения информационной безопасности.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Документоведение», «Программно-аппаратные средства защиты информации», «Организационное и правовое обеспечение информационной безопасности», «Основы информационной безопасности», «Информационные технологии».

Полученные знания, навыки и умения используются при изучении дисциплин старших курсов, при прохождении производственной и преддипломной практик 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

6 семестр

ОК-4. Способность использовать основы правовых знаний в различных сферах деятельности

| Этап (уровень) освоения | Планируемые результаты обучения (показатели) | Критерии оценивания результатов обучения (зачет) |           |
|-------------------------|--|--|-----------|
|                         |  | «Не зачтено»                                     | «Зачтено» |
|                         |  |  |           |

| компетенци<br>и          | достижения<br>заданного уровня<br>освоения<br>компетенций)   |  |   |
|--------------------------|--|--|---|
| Первый этап<br>(уровень) | 1. Знать основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, процесс становления систем защиты информации в ведущих зарубежных странах, особенности государственной политики в области защиты информации, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности | Фрагментарные представления о понятиях, целях, принципах, сферах применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, процесс становления систем защиты информации в ведущих зарубежных странах, особенности государственной политики в области защиты информации, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности | Сформированные, но содержащие отдельные неточности о понятиях, целях, принципах, сферах применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, процесс становления систем защиты информации в ведущих зарубежных странах, особенности государственной политики в области защиты информации, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности |
| Второй этап<br>(уровень) | 1. Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности   | Фрагментарное умение ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности   | В целом успешное, но содержащее отдельные пробелы ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности   |
| Третий этап<br>(уровень) | 1. Владеть навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности   | Фрагментарное владение навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности   | В целом успешное, но содержащее отдельные пробелы владения навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности  |

ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

| Этап (уровень) освоения компетенции и | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)   | Критерии оценивания результатов обучения (зачет)  |   |
|---------------------------------------|---|---|---|
|                                       |   | «Не зачтено»  | «Зачтено»   |
| Первый этап (уровень)                 | Знать нормативные документы для обоснования безопасности конфиденциальной информации в информационных системах, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, достижения международного опыта организации и совершенствования систем защиты информации | Фрагментарно знает основные документы для обоснования безопасности конфиденциальной информации в информационных системах, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, достижения международного опыта организации и совершенствования систем защиты информации | Уверенно знает основные документы для обоснования безопасности конфиденциальной информации в информационных системах, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, достижения международного опыта организации и совершенствования систем защиты информации |
| Второй этап (уровень)                 | Уметь собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности                                       | Не показывает сформированные умения собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности                   | Уверенно использует приемы работ по сбору, анализу и интерпретации необходимой информации, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности                           |



|                       |   |   |   |
|-----------------------|---|---|---|
| Третий этап (уровень) | Владеть навыками сбора и обработки необходимых данных; навыками анализа и интерпретации содержащейся в различных источниках информации, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, иметь представление о международных стандартах безопасности, включая стратегии их мониторинга и аудита, определения целей, уровней безопасности и их важности. | Не владеет основными навыками сбора и обработки необходимых данных; навыками анализа и интерпретации содержащейся в различных источниках информации, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, иметь представление о международных стандартах безопасности, включая стратегии их мониторинга и аудита, определения целей, уровней безопасности и их важности | Уверенно владеет основными навыками сбора и обработки необходимых данных; навыками анализа и интерпретации содержащейся в различных источниках информации, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, иметь представление о международных стандартах безопасности, включая стратегии их мониторинга и аудита, определения целей, уровней безопасности и их важности |
|-----------------------|---|---|---|

ПСК-1. Способность участвовать в разработке подсистемы управления информационной безопасностью

| Этап (уровень) освоения компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)   | Критерии оценивания результатов обучения (зачет)   |   |
|-------------------------------------|---|--|---|
|                                     |   | «Не зачтено»   | «Зачтено»   |
| Первый этап (уровень)               | Знать технологии обеспечения защиты и сохранности конфиденциальных документов, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, правовые и организационные основы защиты информации в ведущих зарубежных | Фрагментарно знает технологии обеспечения защиты и сохранности конфиденциальных документов, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, правовые и организационные основы защиты информации в ведущих зарубежных странах тенденции и перспективы развития международного сотрудничества в данной | Уверенно знает основные технологии обеспечения защиты и сохранности конфиденциальных документов, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, правовые и организационные основы защиты информации в ведущих зарубежных странах тенденции и перспективы развития международного сотрудничества в данной |

|                       |   |   |  |
|-----------------------|---|---|--|
|                       | странах тенденции и перспективы развития международного сотрудничества в данной области   | области   | области  |
| Второй этап (уровень) | Уметь конфигурировать и использовать средства защиты информации в ОС и прикладных программах, настраивать антивирусные программы и другие средства борьбы с программными закладками, применять технические средства защиты данных, проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам. | Не показывает сформированные умения конфигурировать и использовать средства защиты информации в ОС и прикладных программах, настраивать антивирусные программы и другие средства борьбы с программными закладками, применять технические средства защиты данных, проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам. | Уверенно умеет конфигурировать и использовать средства защиты информации в ОС и прикладных программах, настраивать антивирусные программы и другие средства борьбы с программными закладками, применять технические средства защиты данных, проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам. |
| Третий этап (уровень) | Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий  | Не владеет навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий   | Уверенно владеет навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий  |

ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью

| Этап (уровень) освоения компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)  | Критерии оценивания результатов обучения (зачет)  |  |
|-------------------------------------|--|---|--|
|                                     |  | «Не зачтено»  | «Зачтено»  |
| Первый этап (уровень)               | Знать состояние законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; | Фрагментарно знает состояние законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным | Знает основы состояния законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, |

|                       |  |  |   |
|-----------------------|--|--|---|
|                       | аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах  | обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах  | тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах  |
| Второй этап (уровень) | Уметь: обосновывать организационно-технические мероприятия по защите информации.   | Не показывает сформированные умения обосновывать организационно-технические мероприятия по защите информации   | Уверенно использует большинство методов обосновывать организационно-технические мероприятия по защите информации  |
| Третий этап (уровень) | Владеть: навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности; эксплуатации современного электронного оборудования и информационно-коммуникационных технологий | Не владеет основными навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности; эксплуатации современного электронного оборудования и информационно-коммуникационных технологий | Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности; эксплуатации современного электронного оборудования и информационно-коммуникационных технологий |

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей дисциплины, 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).

#### 7 семестр

ОК-4. Способность использовать основы правовых знаний в различных сферах деятельности

| Этап (уровень) освоения компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций) | Критерии оценивания результатов обучения (экзамен) |                                    |                               |                              |
|-------------------------------------|---|--|------------------------------------|-------------------------------|------------------------------|
|                                     |   | 2 («Не удовлетворительно»)                         | 3 («Удовлетворительно»)            | 4 («Хорошо»)                  | 5 («Отлично»)                |
| Первый этап (уровень)               | 1. Знать основные понятия, цели,  | Фрагментарные представления                        | Неполные представления о понятиях, | Сформированные, но содержащие | Сформированные представления |

|                              |  |   |   |  |   |
|------------------------------|--|---|---|--|---|
|                              | <p>принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, процесс становления систем защиты информации в ведущих зарубежных странах, особенности государственной политики в области защиты информации, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности</p> | <p>о понятиях, целях, принципах, сферах применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, процесс становления систем защиты информации в ведущих зарубежных странах, особенности государственной политики в области защиты информации, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности</p> | <p>целях, принципах, сферах применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, процесс становления систем защиты информации в ведущих зарубежных странах, особенности государственной политики в области защиты информации, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности</p> | <p>отдельные неточности о понятиях, целях, принципах, сферах применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, процесс становления систем защиты информации в ведущих зарубежных странах, особенности государственной политики в области защиты информации, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности</p> | <p>о понятиях, целях, принципах, сферах применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, процесс становления систем защиты информации в ведущих зарубежных странах, особенности государственной политики в области защиты информации, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности</p> |
| <p>Второй этап (уровень)</p> | <p>1. Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности</p>  | <p>Фрагментарное умение ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности</p>   | <p>В целом успешное, но не систематическое умение ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и</p>  | <p>В целом успешное, но содержащее отдельные пробелы ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и</p>  | <p>Сформированное умение ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности</p>  |

|                       |  |   |   |   |  |
|-----------------------|--|---|---|---|--|
|                       |  |   | использовать их в своей деятельности  | использовать их в своей деятельности  |  |
| Третий этап (уровень) | 1. Владеть навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности | Фрагментарное владение навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующим и федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности | В целом успешное, но не систематическое владение навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующим и федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности | В целом успешное, но содержащее отдельные пробелы владения навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующим и федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности | Успешное и систематическое владение навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующим и федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности |

ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

| Этап (уровень) освоения компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)      | Критерии оценивания результатов обучения (экзамен)                                  |  |  |   |
|-------------------------------------|--|---|--|--|---|
|                                     |  | 2 («Не удовлетворительно»)  | 3 («Удовлетворительно»)  | 4 («Хорошо»)   | 5 («Отлично»)   |
| Первый этап (уровень)               | Знать нормативные документы для обоснования конфиденциальной информации в информационных системах, | Фрагментарно знает основные документы для обоснования конфиденциальной информации в | В целом знает основные документы для обоснования конфиденциальной информации в | Знает основные документы для обоснования конфиденциальной информации в | Уверенно знает основные документы для обоснования конфиденциальной информации в |

|                       |   |   |  |  |   |
|-----------------------|---|---|--|--|---|
|                       | на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, достижения международного опыта организации и совершенствования систем защиты информации   | информационных системах, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, достижения международного опыта организации и совершенствования систем защиты информации  | ных системах, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, достижения международного опыта организации и совершенствования систем защиты информации  | ных системах, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, достижения международного опыта организации и совершенствования систем защиты информации  | информационных системах, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, достижения международного опыта организации и совершенствования систем защиты информации  |
| Второй этап (уровень) | Уметь собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности | Не показывает сформированные умения собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности | Умеет использовать некоторые приемы работ по сбору, анализу и интерпретации и необходимой информации, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности | Уверенно использует большинство приемов работ по сбору, анализу и интерпретации и необходимой информации, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности | Уверенно использует приемы работ по сбору, анализу и интерпретации и необходимой информации, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности |

|                       |   |   |   |  |   |
|-----------------------|---|---|---|--|---|
|                       |   | деятельности  | деятельности  | деятельности   |   |
| Третий этап (уровень) | Владеть навыками сбора и обработки необходимых данных; навыками анализа и интерпретации содержащейся в различных источниках информации, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, иметь представление о международных стандартах безопасности, включая стратегии их мониторинга и аудита, определения целей, уровней безопасности и их важности. | Не владеет основными навыками сбора и обработки необходимых данных; навыками анализа и интерпретации и содержащейся в различных источниках информации, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, иметь представление о международных стандартах безопасности, включая стратегии их мониторинга и аудита, определения целей, уровней безопасности и их важности | Владеет основными навыками сбора и обработки необходимых данных; навыками анализа и интерпретации и содержащейся в различных источниках информации, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, иметь представление о международных стандартах безопасности, включая стратегии их мониторинга и аудита, определения целей, уровней безопасности и их важности, но допускает ошибки | Владеет основными навыками сбора и обработки необходимых данных; навыками анализа и интерпретации и содержащейся в различных источниках информации, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, иметь представление о международных стандартах безопасности, включая стратегии их мониторинга и аудита, определения целей, уровней безопасности и их важности | Уверенно владеет основными навыками сбора и обработки необходимых данных; навыками анализа и интерпретации и содержащейся в различных источниках информации, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, иметь представление о международных стандартах безопасности, включая стратегии их мониторинга и аудита, определения целей, уровней безопасности и их важности |

ПСК-1. Способность участвовать в разработке подсистемы управления информационной безопасностью

| Этап (уровень) | Планируемые результаты | Критерии оценивания результатов обучения (экзамен) |   |              |               |
|----------------|------------------------|--|---|--------------|---------------|
|                |                        | 2 («Не   | 3 | 4 («Хорошо») | 5 («Отлично») |

| освоения компетенции  | обучения (показатели достижения заданного уровня освоения компетенций)  | удовлетворительно»)»)  | («Удовлетворительно»)»)  |  |   |
|-----------------------|---|--|--|--|---|
| Первый этап (уровень) | Знать технологии обеспечения защиты и сохранности конфиденциальных документов, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, правовые и организационные основы защиты информации в ведущих зарубежных странах тенденции и перспективы развития международного сотрудничества в данной области | Фрагментарно знает технологии обеспечения защиты и сохранности конфиденциальных документов, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, правовые и организационные основы защиты информации в ведущих зарубежных странах тенденции и перспективы развития международного сотрудничества в данной области | В целом знает основные технологии обеспечения защиты и сохранности конфиденциальных документов, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, правовые и организационные основы защиты информации в ведущих зарубежных странах тенденции и перспективы развития международного сотрудничества в данной области | Знает основные технологии обеспечения защиты и сохранности конфиденциальных документов, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, правовые и организационные основы защиты информации в ведущих зарубежных странах тенденции и перспективы развития международного сотрудничества в данной области | Уверенно знает основные технологии обеспечения защиты и сохранности конфиденциальных документов, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, правовые и организационные основы защиты информации в ведущих зарубежных странах тенденции и перспективы развития международного сотрудничества в данной области |
| Второй этап (уровень) | Уметь конфигурировать и использовать средства защиты информации в ОС и прикладных программах, настраивать антивирусные  | Не показывает сформированные умения конфигурировать и использовать средства защиты информации в ОС и прикладных программах,  | Умеет использовать некоторые методы конфигурировать и использовать средства защиты информации в ОС и прикладных  | Уверенно использует большинство методов конфигурировать и использовать средства защиты информации в ОС и прикладных  | Уверенно умеет конфигурировать и использовать средства защиты информации в ОС и прикладных программах, настраивать  |



|                       |  |  |  |  |  |
|-----------------------|--|--|--|--|--|
|                       | программы и другие средства борьбы с программными закладками, применять технические средства защиты данных, проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам. | настраивать антивирусные программы и другие средства борьбы с программным и закладками, применять технические средства защиты данных, проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам. | программах, настраивать антивирусные программы и другие средства борьбы с программным и закладками, применять технические средства защиты данных, проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам. | программах, настраивать антивирусные программы и другие средства борьбы с программным и закладками, применять технические средства защиты данных, проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам. | антивирусные программы и другие средства борьбы с программным и закладками, применять технические средства защиты данных, проводить анализ защищённости объектов и определять класс защиты информации по международным стандартам. |
| Третий этап (уровень) | Владеть навыками эксплуатации современного электронного оборудования и информационных технологий   | Не владеет навыками эксплуатации современного электронного оборудования и информационных технологий  | Владеет основными навыками эксплуатации современного электронного оборудования и информационных технологий, но допускает значительные ошибки.  | Владеет основными навыками эксплуатации современного электронного оборудования и информационных технологий   | Уверенно владеет навыками эксплуатации современного электронного оборудования и информационных технологий  |

ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью

| Этап (уровень) освоения компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций) | Критерии оценивания результатов обучения (экзамен) |                         |                        |                |
|-------------------------------------|---|--|-------------------------|------------------------|----------------|
|                                     |   | 2 («Не удовлетворительно»)                         | 3 («Удовлетворительно») | 4 («Хорошо»)           | 5 («Отлично»)  |
| Первый этап                         | Знать состояние   | Фрагментарно знает                                 | В целом знает состояние | Знает основы состояния | Уверенно знает |

|                       |  |  |  |  |  |
|-----------------------|--|--|--|--|--|
| (уровень)             | законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах | состояние законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах | законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах | законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах | состояние законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах |
| Второй этап (уровень) | Уметь: обосновывать организационно-технические мероприятия по защите информации.   | Не показывает сформированные умения обосновывать организационно-технические мероприятия по защите информации   | Умеет использовать некоторые методы обосновывать организационно-технические мероприятия по защите информации   | Уверенно использует большинство методов обосновывать организационно-технические мероприятия по защите информации   | Уверенно умеет обосновывать организационно-технические мероприятия по защите информации  |
| Третий этап (уровень) | Владеть: навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности; эксплуатации  | Не владеет основными навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности;   | Владеет основными навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности;  | Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности; эксплуатации   | Уверенно владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности;   |

|  |  |   |  |  |   |
|--|--|---|--|--|---|
|  | современного электронного оборудования и информационных технологий | эксплуатации современного электронного оборудования и информационных технологий | эксплуатации современного электронного оборудования и информационных технологий, но допускает значительные ошибки. | современного электронного оборудования и информационных технологий | эксплуатации современного электронного оборудования и информационных технологий |
|--|--|---|--|--|---|

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей дисциплины, перечисленных в рейтинг-плане дисциплины, для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10.

Шкалы оценивания для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

**4.2. Типовые контрольные задания или иные материалы, необходимые для 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 этап<br>Знания | Знать основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, процесс становления систем защиты информации в ведущих зарубежных странах, особенности государственной политики в области защиты информации, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности | ОК-4. Способность использовать основы правовых знаний в различных сферах деятельности   | Письменная контрольная работа, Практическая работа. |
|                  | Знать нормативные документы для обоснования безопасности конфиденциальной информации в информационных системах, на объектах информатизации, информационно-аналитического и  | ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по | Письменная контрольная работа, Практическая работа. |

|                  |   |   |   |
|------------------|---|---|---|
|                  | информационно-психологического обеспечения правоохранительной деятельности, достижения международного опыта организации и совершенствования систем защиты информации  | вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности   |   |
|                  | Знать технологии обеспечения защиты и сохранности конфиденциальных документов, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, правовые и организационные основы защиты информации в ведущих зарубежных странах тенденции и перспективы развития международного сотрудничества в данной области | ПСК-1. Способность участвовать в разработке подсистемы управления информационной безопасностью  | Письменная контрольная работа, Практическая работа. |
|                  | Знать состояние законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах  | ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью   | Письменная контрольная работа, Практическая работа. |
| 2 этап<br>Умения | Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности   | ОК-4. Способность использовать основы правовых знаний в различных сферах деятельности   | Письменная контрольная работа, Практическая работа. |
|                  | Уметь собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности   | ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности | Письменная контрольная работа, Практическая работа. |
|                  | Уметь конфигурировать и использовать средства защиты информации в ОС и прикладных программах, настраивать антивирусные программы и другие средства борьбы с программными закладками, применять технические средства защиты данных, проводить анализ защищённости объектов и определять класс защиты информации по   | ПСК-1. Способность участвовать в разработке подсистемы управления информационной безопасностью  | Письменная контрольная работа, Практическая работа. |

|                          |   |   |   |
|--------------------------|---|---|---|
|                          | международным стандартам.   |   |   |
|                          | Уметь обосновывать организационно-технические мероприятия по защите информации.   | ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью   | Письменная контрольная работа, Практическая работа. |
| 3 этап Владения навыками | Владеть навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности   | ОК-4. Способность использовать основы правовых знаний в различных сферах деятельности   | Письменная контрольная работа, Практическая работа. |
|                          | Владеть навыками сбора и обработки необходимых данных; навыками анализа и интерпретации содержащейся в различных источниках информации, на объектах информатизации, информационно-аналитического и информационно-психологического обеспечения правоохранительной деятельности, иметь представление о международных стандартах безопасности, включая стратегии их мониторинга и аудита, определения целей, уровней безопасности и их важности. | ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности | Письменная контрольная работа, Практическая работа. |
|                          | Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий  | ПСК-1. Способность участвовать в разработке подсистемы управления информационной безопасностью  | Письменная контрольная работа, Практическая работа. |
|                          | Владеть навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности; эксплуатации современного электронного оборудования и информационно-коммуникационных технологий   | ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью   | Письменная контрольная работа, Практическая работа. |

### 4.3. Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в приложении 2.

Типовые вопросы для зачета 6 семестр

1. Назовите основные этапы развития методов и средств ЗИ в процессе эволюции человечества.
2. Назовите особенности второго периода развития методов и средств ЗИ.
3. Каковы основные виды носителей информации?

4. На какой период приходится наиболее интенсивное решение проблем информационной безопасности?
5. Охарактеризуйте современное состояние проблемы защиты информации в мире.
6. Что понимается под защитой информации?
7. Назовите основные элементы типовой системы защиты информации.
8. Охарактеризуйте картину политических отношений в современном мире.
9. Назовите причины, вызвавшие появление информационных войн.
10. В чем состоит сущность информационного воздействия?
11. Назовите сферы деятельности человечества, в которых возможно применение технологии информационных войн для достижения поставленных задач.
12. Дайте определение понятию «информационная война».
13. Назовите основные виды информационной войны.
14. В чем состоят цели информационной войны?
15. Дайте определение понятию «информационное оружие» и назовите основные виды информационного оружия.
16. Назовите уровни концепции ИВ США. В чем их основные отличия?
17. Что представляет собой военный уровень концепции ИВ США?
18. Назовите основные принципы ИВ, реализуемые на военном уровне концепции ИВ США.
19. Назовите основные формы ИВ. Кратко их охарактеризуйте.
20. Какова основная цель Закона «Об информационной безопасности» в США?
21. Назовите нормативно-правовые акты, регулирующие правовое обеспечение ИВ в США.
22. Каковы особенности подготовки кадров в области ИВ в США?

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей дисциплины, перечисленных в рейтинг-плане дисциплины, для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10.

Шкалы оценивания для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

#### Экзамен

##### Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов

##### Типовые экзаменационные материалы

##### Вопросы к экзамену 7 семестр

1. История развития проблемы защиты информации
2. Современное состояние проблемы защиты информации
3. Структура систем защиты информации, применяемых в общемировой практике обеспечения информационной безопасности
4. Типовая система защиты информации
5. Современная картина международных отношений в мире
6. Основы информационно-психологического воздействия.
7. Информационная война
8. Информационное противоборство
9. Типы информационного оружия
10. Уровни реализации концепции информационной войны в США
11. Правовое регулирование информационной безопасности в США

12. Государственные органы обеспечения национальной безопасности США
13. Агентство национальной безопасности США
14. Центральное разведывательное управление США
15. Министерство обороны США
16. Национальный фонд знаний США
17. Национальная ассоциация компьютерной безопасности США
18. Особенности подготовки кадров в области информационной безопасности в США
19. Состояние проблемы информационной безопасности в странах Евросоюза
20. Системы защиты информации в Великобритании
21. Разведывательная служба Великобритании
22. Контрразведывательная служба Великобритании
23. Системы защиты информации в Германии
24. Федеральная разведывательная служба Германии. Федеральная служба безопасности в сфере информационной техники
25. Федеральное бюро защиты конституции Германии
26. Системы защиты информации во Франции
27. Структура спецслужб Франции
28. Системы защиты информации в Швеции
29. Структура спецслужб Швеции
30. Особенности работы промышленных служб безопасности Швеции
31. Представление об информационном противоборстве в КНР
32. Законодательство в сфере информационной безопасности в КНР
33. Организационная структура спецслужб КНР
34. «Великая стена» информационной безопасности КНР
35. Развитие международного сотрудничества в области информационной безопасности
36. Окинавская хартия глобального информационного общества
37. Токийская декларация
38. Международные организации в области информационной безопасности
39. Ассоциация аудита и контроля информационных систем
40. Центр интернет-безопасности
41. Интернет-союз информационной безопасности
42. Правовое регулирование сети Интернет
43. Предпосылки создания стандартов информационной безопасности
44. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга)
45. Гармонизированные критерии европейских стран
46. Германский стандарт BS 1
47. Британский стандарт BS 7799
48. Международный стандарт ISO 17799
49. Международный стандарт ISO 15408 «Общий критерий»
50. Стандарт COBIT
51. Практика компании IBM в области защиты информации
52. Практика компании CiscoSystems в разработке сетевой политики безопасности
53. Практика компании Microsoft в области информационной безопасности

Пример экзаменационного билета

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  
Системы защиты информации в ведущих зарубежных странах  
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1

1. Структура спецслужб Франции
2. Британский стандарт BS 7799

Зав. кафедрой УИБ

А.С. Исмагилова  
Кафедра управления информационной безопасностью

---

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  
Системы защиты информации в ведущих зарубежных странах  
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №2

1. Международные организации в области информационной безопасности
1. Организационная структура спецслужб КНР

Зав. кафедрой УИБ

А.С. Исмагилова  
Кафедра управления информационной безопасностью

---

Перевод оценки из 100-балльной в четырехбалльную производится следующим образом:

- 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 ответа на экзамене

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. 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. Студент не смог ответить ни на один дополнительный вопрос.

### **Комплект контрольных работ**

Для контроля освоения и/или расширения знаний, умений, владений предусмотрены несколько контрольных работ.

#### **Модуль 1.**

Общая характеристика систем защиты в ведущих зарубежных странах

Письменная контрольная работа №1

Защита информации в США

#### **Вопросы**

1. Информационное противоборство в современном мире.
2. Центральное разведывательное управление США.
3. Подготовка специалистов в области информационной безопасности в США?

#### **Критерии оценки**

| Показатель оценки    | Распределение баллов |
|----------------------|----------------------|
| Выполнены пункты 1-2 | 15                   |
| Выполнены пункты 1-3 | 25                   |
| Максимальный балл    | 25                   |

#### **Модуль 2.**

Системы защиты информации в западных странах

Письменная контрольная работа №2

Защита информации в ведущих европейских странах

#### **Вопросы**

1. Каковы особенности работы промышленных служб безопасности Швеции?
2. Какова, по мнению руководства Германии, главная причина повышения уязвимости сведений составляющих коммерческую тайну?
3. Какое ведомство в Великобритании и как следит за соблюдением законов о защите информации и защите персональных данных?

#### **Критерии оценки**

| Показатель оценки    | Распределение баллов |
|----------------------|----------------------|
| Выполнены пункты 1-2 | 15                   |
| Выполнены пункты 1-3 | 25                   |
| Максимальный балл    | 25                   |

#### **Модуль 3.**

Системы защиты информации в восточных странах

Письменная контрольная работа №3

Защита информации в ведущих азиатских странах

#### **Вопросы**

1. «Великая стена» информационной безопасности КНР.

2. Представление об информационном противоборстве в КНР
3. Система защиты информации в Японии

#### Критерии оценки

| Показатель оценки    | Распределение баллов |
|----------------------|----------------------|
| Выполнены пункты 1-2 | 8                    |
| Выполнены пункты 1-3 | 15                   |
| Максимальный балл    | 15                   |

#### Модуль 4.

Международные нормативно-правовые акты и стандарты в области ЗИ  
Письменная контрольная работа №4

Международное сотрудничество в области информационной безопасности

#### Вопросы

1. Развитие международного сотрудничества в области информационной безопасности
2. Международные организации в области информационной безопасности
3. Международный стандарт ISO 17799

#### Критерии оценки

| Показатель оценки    | Распределение баллов |
|----------------------|----------------------|
| Выполнены пункты 1-2 | 8                    |
| Выполнены пункты 1-3 | 15                   |
| Максимальный балл    | 15                   |

#### Комплект практических заданий

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических заданий.

#### Модуль 1.

Общая характеристика систем защиты в ведущих зарубежных странах

Типовое практическое задание 1

Задание 1. Информационные войны

1. Привести примеры информационно-психологического воздействия.
2. Проанализировать информационные войны в истории.
3. Выявить основные особенности ведения информационных войн в наше время.

#### Методические указания

а. В первую очередь необходимо обратить внимание на особенности системы защиты государственной тайны, коммерческой тайны и персональных данных в выбранной стране.

б. Помнить, что в каждой стране может быть собственная терминология, т.е. речь можно вести только об аналогах.

в. Поощряется наличие сравнительного анализа с аналогами в России.

#### Критерии оценки

| Показатель оценки    | Распределение баллов |
|----------------------|----------------------|
| Выполнены пункты 1-2 | 10                   |
| Выполнены пункты 1-3 | 15                   |
| Максимальный балл    | 15                   |

## Модуль 2.

### Системы защиты информации в западных странах

#### Типовое практическое задание 2

Задание 2 Особенности защиты информации в отдельно взятой стране Европейского или Американского континента

1. Ознакомиться с краткой историей произвольно выбранного государства Европейского или Американского континента.
2. Собрать сведения по защите информации в этой стране.
3. Проанализировать собранную информацию и подготовить доклад.

#### Методические указания

- а. В первую очередь необходимо обратить внимание на особенности системы защиты государственной тайны, коммерческой тайны и персональных данных в выбранной стране.
- б. Помнить, что в каждой стране может быть собственная терминология, т.е. речь можно вести только об аналогах.
- в. Поощряется наличие сравнительного анализа с аналогами в России.

#### Критерии оценки

| Показатель оценки    | Распределение баллов |
|----------------------|----------------------|
| Выполнены пункты 1-2 | 10                   |
| Выполнены пункты 1-3 | 15                   |
| Максимальный балл    | 15                   |

## Модуль 3.

### Системы защиты информации в восточных странах

#### Типовое практическое задание 3

Задание 3. Особенности защиты информации в отдельно взятой стране Азии или Африки

1. Ознакомиться с краткой историей произвольно выбранной страны Азии или Африки.
2. Собрать сведения по защите информации в этой стране.
3. Проанализировать собранную информацию и подготовить доклад.

#### Методические указания

- а. В первую очередь необходимо обратить внимание на особенности системы защиты государственной тайны, коммерческой тайны и персональных данных в выбранной стране.
- б. Помнить, что в каждой стране может быть собственная терминология, т.е. речь можно вести только об аналогах.
- в. Поощряется наличие сравнительного анализа с аналогами в России.

#### Критерии оценки

| Показатель оценки    | Распределение баллов |
|----------------------|----------------------|
| Выполнены пункты 1-2 | 8                    |
| Выполнены пункты 1-3 | 14                   |
| Максимальный балл    | 14                   |

## Модуль 4.

### Международные нормативно-правовые акты и стандарты в области ЗИ

#### Типовое практическое задание 4

## Классификация подходов к защите информации в мире

1. Провести классификацию подходов к защите государственной тайны в странах мира на основе анализа полученной информации из предыдущих практических заданий и письменных контрольных работ.
2. Провести классификацию подходов к защите коммерческой тайны в странах мира на основе анализа полученной информации из предыдущих практических заданий и письменных контрольных работ.
3. Провести классификацию подходов к защите персональных данных в странах мира на основе анализа полученной информации из предыдущих практических заданий и письменных контрольных работ.

### Критерии оценки

| Показатель оценки    | Распределение баллов |
|----------------------|----------------------|
| Выполнены пункты 1-2 | 8                    |
| Выполнены пункты 1-3 | 14                   |
| Максимальный балл    | 14                   |

## 5. Учебно-методическое и информационное обеспечение дисциплины

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

#### Основная литература

1. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Издательство «Флинта», 2016. - 224 с. - (Организация и технология защиты информации). - Библиогр.: с. 192-193. - ISBN 978-5-9765-1274-0 ; То же [Электронный ресурс]. - URL: [http://biblioclub.ru/index.php?page=book&id=93351\(17.01.2019\)](http://biblioclub.ru/index.php?page=book&id=93351(17.01.2019))
2. 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> (17.01.2019).
3. Смирнов, А.А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза : монография / А.А. Смирнов. - Москва : ЮНИТИ-ДАНА: Закон и право, 2012. - 159 с. : ил. - (Научные издания для юристов). - Библиогр. в кн. - ISBN 978-5-238-02259-8 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=448202> (17.01.2019).
4. Савельев, А.И. Электронная коммерция в России и за рубежом: правовое регулирование : монография / А.И. Савельев. - Москва : Статут, 2014. - 543 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-8354-1018-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=448075> (18.01.2019).
5. Вирен, Г. Современные медиа: приемы информационных войн : учебное пособие / Г. Вирен. - Москва : Аспект Пресс, 2017. - 127 с. - Библиогр. в кн. - ISBN 978-5-7567-0824-0 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=457409> (18.01.2019).

#### Дополнительная литература

6. ЛЯН, М. ПРАВОВАЯ ЗАЩИТА КОММЕРЧЕСКОЙ ТАЙНЫ В КИТАЕ. [Электронный ресурс] — Электрон. дан. // Вестник Бурятского государственного университета. — 2014. — № 2. — С. 283-285. — Режим доступа: <http://e.lanbook.com/journal/issue/292818> — Загл. с экрана.
7. Комиссарова, Е.А. ОСНОВНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ [Электронный ресурс] / Е.А. Комиссарова, Е.А. Комиссаров. // Научные записки ОрелГИЭТ. — Электрон. дан. — 2015. — № 1. — С. 348-352. — Режим доступа: <https://e.lanbook.com/journal/issue/301385>. — 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/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/matematika/> – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. [www.newlibrary.ru](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. [www.nehudlit.ru](http://www.nehudlit.ru) – Электронная библиотека учебных материалов.
13. 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.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

| Наименование специализированных аудиторий, кабинетов, лабораторий  | Вид занятий  | Наименование оборудования, программного обеспечения  |
|--|--|--|
| <b>1. учебная аудитория для проведения занятий лекционного типа:</b><br>аудитория № 403 (гуманитарный корпус), аудитория № 405 | Лекции, практические занятия, групповые и индивидуальные консультации, текущий контроль, | <b>Аудитория № 403</b><br>Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. |
|  |  | <b>Аудитория № 405</b><br>Учебная мебель, доска, вокальные радиомикрофоны  |

|   |                                 |   |
|---|---------------------------------|---|
| <p>(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 занятий семинарского типа:</b></p> <p>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>3. учебная аудитория для проведения групповых и индивидуальных консультаций:</b></p> <p>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</p> | <p>промежуточная аттестация</p> | <p>AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNT EST -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></p> <p>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></p> <p>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></p> <p>Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p><b>Аудитория № 418</b></p> <p>Учебная мебель, доска, Экран настенный Lumien Master Piktur 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.</p> <p><b>Аудитория № 419</b></p> <p>Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p><b>Аудитория № 515</b></p> <p>Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром.</p> <p><b>Аудитория № 516</b></p> <p>Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p><b>Аудитория № 509</b></p> <p>Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 608</b></p> <p>Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 609</b></p> <p>Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 610</b></p> <p>Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-</p> |
|---|---------------------------------|---|

|   |  |   |
|---|--|---|
| <p>аудитория № 420 (гуманитарный корпус).</p> <p><b>4. 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>5. помещения для самостоятельной работы:</b> аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).</p> |  | <p>HDH(m)ver14,10м.</p> <p><b>Аудитория № 613</b></p> <p>Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p><b>Компьютерный класс аудитория № 420</b></p> <p>Учебная мебель, моноблоки стационарные 15 шт.</p> <p><b>Компьютерный класс аудитория № 404</b></p> <p>Учебная мебель, компьютеры -15 штук.</p> <p><b>Аудитория 402 читальный зал библиотеки</b></p> <p>Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные</p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</li> <li>3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.</li> </ol> |
|---|--|---|

## Приложение 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Содержание рабочей программы дисциплины  
Системы защиты информации в ведущих зарубежных странах

на 6 семестр

| Вид работы  | Объем дисциплины     |
|---|----------------------|
|   | Очная форма обучения |
| Общая трудоемкость дисциплины (ЗЕТ / часов)   | 2 ЗЕТ / 72 часа      |
| Учебных часов на контактную работу с преподавателем:  | 32,2                 |
| лекций  | 16                   |
| практических / семинарских  | 16                   |
| лабораторных  | -                    |
| других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) | 0,2                  |
| Учебных часов на самостоятельную работу   | 39,8                 |
| Учебных часов на подготовку к зачету  |                      |

Форма контроля  
Зачет 6 семестр



| № | Тема и содержание  | Форма изучения материалов:<br>лекции, практические занятия, семинарские занятия,<br>лабораторные работы, самостоятельная работа и<br>трудоемкость (в часах) |             |    |     | Основная и<br>дополнительна<br>я литература,<br>рекомендуемая<br>студентам<br>(номера из<br>списка) | Задания по<br>самостоятельной<br>работе студентов | Форма текущего<br>контроля<br>успеваемости<br>(коллоквиумы,<br>контрольные<br>работы,<br>компьютерные<br>тесты и т.п.) |   |
|---|--|---|-------------|----|-----|---|---|--|---|
|   |  | ЛК  | ПР /<br>Сем | ЛР | СРС |   |   |  |   |
| 1 | 2  | 3   | 4           | 5  | 6   | 7   | 8   | 9  | 10  |
| 1 | <b>Общая характеристика систем защиты в ведущих зарубежных странах</b> |   | 2           | 2  |     | 5   | 1-7   | Провести сравнительный общий анализ развития систем защиты информации в зарубежных странах и России                    | Письменная контрольная работа,<br>Практическая работа |
| 2 | История развития систем защиты информации в зарубежных странах         |   | 2           | 2  |     | 5   | 1-7   | Провести сравнительный анализ истории систем защиты информации в зарубежных странах и России                           | Письменная контрольная работа,<br>Практическая работа |
| 3 | Информационное противоборство в мире                                   |   | 2           | 2  |     | 5   | 1-6   | Провести сравнительный анализ информационного противоборства зарубежных стран и России                                 | Письменная контрольная работа,<br>Практическая работа |
| 4 | Информационное противоборство в системе международных отношений        |   | 2           | 2  |     | 5   | 1-7   | Провести сравнительный анализ информационного  | Письменная контрольная работа,<br>Практическая        |

|   |   |  |    |    |  |      |  |  |  |
|---|---|--|----|----|--|------|--|--|--|
|   | современного общества                                 |  |    |    |  |      | противоборства ведущих зарубежных стран и России | работа   |  |
| 5 | <b>Системы защиты информации в западных странах</b>   |  | 2  | 2  |  | 5    | 1-5  | Провести сравнительный анализ истории систем защиты информации в США и России      | Письменная контрольная работа, Практическая работа |
| 6 | Системы защиты информации в США                       |  | 2  | 2  |  | 5    | 1-6  | Провести сравнительный анализ современных систем защиты информации в США и России  | Письменная контрольная работа, Практическая работа |
| 7 | Системы защиты информации в Европе                    |  | 2  | 2  |  | 5    | 1-5  | Провести сравнительный анализ истории систем защиты информации Европы и России     | Письменная контрольная работа, Практическая работа |
| 8 | Системы защиты информации в ведущих странах Евросоюза |  | 2  | 2  |  | 4,8  | 1-5  | Провести сравнительный анализ современных систем защиты информации Европы и России | Письменная контрольная работа, Практическая работа |
|   | <b>Итого</b>  |  | 16 | 16 |  | 39,8 |  |  |  |

Системы защиты информации в ведущих зарубежных странах  
на 7 семестр

| Вид работы  | Объем дисциплины     |
|---|----------------------|
|   | Очная форма обучения |
| Общая трудоемкость дисциплины (ЗЕТ / часов)   | 4 ЗЕТ / 144 часа     |
| Учебных часов на контактную работу с преподавателем:  | 37,2                 |
| лекций  | 18                   |
| практических / семинарских  | 18                   |
| лабораторных  | -                    |
| других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) | 1,2                  |
| Учебных часов на самостоятельную работу   | 72                   |
| Учебных часов на подготовку к экзамену / зачету   | 34,8                 |

Форма контроля  
Экзамен 7 семестр

| № | Тема и содержание   | Форма изучения материалов:<br>лекции, практические занятия, семинарские занятия,<br>лабораторные работы, самостоятельная работа и<br>трудоемкость (в часах) |          |    |     | Основная и<br>дополнительн<br>ая<br>литература,<br>рекомендуема<br>я студентам<br>(номера из<br>списка) | Задания по<br>самостоятельной работе<br>студентов | Форма<br>текущего<br>контроля<br>успеваемости<br>(коллоквиумы,<br>контрольные<br>работы,<br>компьютерные<br>тесты и т.п.) |   |
|---|---|---|----------|----|-----|---|---|---|---|
|   |   | ЛК  | ПР / Сем | ЛР | СРС |   |   |   |   |
| 1 | 2   | 3   | 4        | 5  | 6   | 7   | 8   | 9   | 10  |
| 3 | <b>Системы защиты информации в восточных странах</b>                  |   | 2        | 2  |     | 9   | 1-6   | Провести анализ международных нормативно-правовые актов и стандартов в области защиты информации                          | Письменная контрольная работа,<br>Практическая работа |
| 2 | История системы защиты информации в Китайской народной республике     |   | 2        | 2  |     | 9   | 1-6   | Провести сравнительный анализ истории систем защиты информации Китая и России   | Письменная контрольная работа,<br>Практическая работа |
| 3 | Современная система защиты информации в Китайской народной республике |   | 2        | 2  |     | 9   | 1-6   | Провести сравнительный анализ современных систем защиты информации Китая и России   | Письменная контрольная работа,<br>Практическая работа |

|   |  |  |    |    |  |    |     |   |  |
|---|--|--|----|----|--|----|-----|---|--|
| 4 | Организация защиты информации в Японии   |  | 2  | 2  |  | 9  | 1-6 | Провести сравнительный анализ современных систем защиты информации Японии и России                                      | Письменная контрольная работа, Практическая работа |
| 5 | <b>Международные нормативно-правовые акты и стандарты в области ЗИ</b>         |  | 2  | 2  |  | 9  | 1-7 | Провести сравнительный анализ международных нормативно-правовых актов и стандартов в области защиты информации и России | Письменная контрольная работа, Практическая работа |
| 6 | Международное сотрудничество в области обеспечения информационной безопасности |  | 2  | 2  |  | 9  | 1-7 | Вклад России в международное сотрудничество в области обеспечения информационной безопасности                           | Письменная контрольная работа, Практическая работа |
| 7 | Стандарты информационной безопасности  |  | 2  | 2  |  | 9  | 1-7 | Провести сравнительный анализ стандартов ИБ и России  | Письменная контрольная работа, Практическая работа |
| 8 | Системы ЗИ в ведущих мировых компаниях   |  | 4  | 4  |  | 9  | 1-7 | Провести сравнительный анализ СЗИ ведущих мировых компаний и России   | Письменная контрольная работа, Практическая работа |
|   | <b>Итого</b>   |  | 18 | 18 |  | 72 | 1-7 |   |  |

### Рейтинг – план дисциплины

Системы защиты информации в ведущих зарубежных странах  
 Направление подготовки 10.03.01 Информационная безопасность  
 Курс 3, семестр 6

| Виды учебной деятельности студентов  | Балл за конкретное задание | Число заданий за семестр | Баллы       |              |
|--|----------------------------|--------------------------|-------------|--------------|
|  |                            |                          | Минимальный | Максимальный |
| <b>Модуль 1. Общая характеристика систем защиты в ведущих зарубежных странах</b> |                            |                          |             |              |
| Текущий контроль   |                            |                          |             |              |
| 1. Аудиторная работа   | 10                         | 1                        | 1           | 10           |
| 2. Практическая работа №1  | 15                         | 1                        | 0           | 15           |
| Рубежный контроль  |                            |                          |             |              |
| 1. Письменная контрольная работа №1  | 25                         | 1                        | 0           | 25           |
| Всего  |                            |                          |             | 50           |
| <b>Модуль 2. Системы защиты информации в западных странах</b>                    |                            |                          |             |              |
| Текущий контроль   |                            |                          |             |              |
| 1. Аудиторная работа   | 10                         | 1                        | 1           | 10           |
| 2. Практическая работа №2  | 15                         | 1                        | 0           | 15           |
| Рубежный контроль  |                            |                          |             |              |
| 1. Письменная контрольная работа №2  | 25                         | 1                        | 0           | 25           |
| Всего  |                            |                          |             | 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  |                            |                          |             |              |

## Рейтинг – план дисциплины

### Системы защиты информации в ведущих зарубежных странах

Направление подготовки 10.03.01 Информационная безопасность

Курс 4, семестр 7

| Виды учебной деятельности студентов  | Балл за конкретное задание | Число заданий за семестр | Баллы       |              |
|--|----------------------------|--------------------------|-------------|--------------|
|  |                            |                          | Минимальный | Максимальный |
| <b>Модуль 3. Системы защиты информации в восточных странах</b>                   |                            |                          |             |              |
| Текущий контроль   |                            |                          |             |              |
| 1. Аудиторная работа   | 6                          | 1                        | 1           | 6            |
| 2. Практическая работа №3  | 14                         | 1                        | 0           | 14           |
| Рубежный контроль  |                            |                          |             |              |
| 1. Письменная контрольная работа №3  | 15                         | 1                        | 0           | 15           |
| Всего  |                            |                          |             | 35           |
| <b>Модуль 4. Международные нормативно-правовые акты и стандарты в области ЗИ</b> |                            |                          |             |              |
| Текущий контроль   |                            |                          |             |              |
| 1. Аудиторная работа   | 6                          | 1                        | 1           | 6            |
| 2. Практическая работа №4  | 14                         | 1                        | 0           | 14           |
| Рубежный контроль  |                            |                          |             |              |
| 1. Письменная контрольная работа №4  | 15                         | 1                        | 0           | 15           |
| Всего  |                            |                          |             | 35           |
| <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           |