

«

»

“ ”

“ ”

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Информационная безопасность и защита государственной тайны

: 17.05.01

: 4, : 7

| | | |
|-----------|---------|----------|
| | | |
| | | 7 |
| 1 | () | 4 |
| 2 | | 144 |
| 3 | , . | 81 |
| 4 | , . | 36 |
| 5 | , . | 0 |
| 6 | , . | 36 |
| 7 | , . | 18 |
| 8 | , . | 2 |
| 9 | , . | 7 |
| 10 | , . | 63 |
| 11 | (, ,) | |
| 12 | | |

(): 17.05.01

1161 12.09.2016 . , : 28.09.2016 .

: 1,

(): 17.05.01

, 7 20.06.2017

, 5 21.06.2017

:

, . . .

:

,

:

. . .

1.

1.1

| | |
|---|--|
| Компетенция ФГОС: ОК.8 способность использовать общеправовые знания в различных сферах деятельности; в части следующих результатов обучения: | |
| 4. | |
| 5. | |
| Компетенция ФГОС: ОПК.2 способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасность и угрозы возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны; в части следующих результатов обучения: | |
| 10. | |
| 11. | |
| 12. | |
| 13. | |
| 14. | |
| 2. | |
| 3. | |
| 4. | |
| 5. | |
| 6. | |
| 7. | |
| 8. | |
| 9. | |

2.

2.1

| | |
|-----------|--|
| (, , ,) | |
|-----------|--|

| | |
|---|-----|
| .2. 10 | |
| 1.Задачи, которые решает комплексная защита конфиденциальной информации | ; ; |
| .2. 11 | |
| 2.задачи, решаемые системой инженерной защиты, службой безопасности объекта и режимно-секретными органами | ; ; |
| 3.Основные методы защиты информации техническими средствами | ; ; |
| .2. 12 | |
| 4.регламентные работы, связанные с комплексным обеспечением информационной безопасности конкретных автоматизированных систем | ; ; |
| .2. 13 | |
| 5.О правилах подбора, приема, увольнения, расстановки кадров с учетом выявленных особенностей характера и поведения сотрудников в коллективе. | ; ; |
| .2. 14 | |
| 6.меры, которыми достигается снижение ущерба от возможной утраты информации; | ; ; |

| | |
|---|---|
| .2. 2 | |
| 7.Сертификации ОТСС, ВТСС, средств защиты информации и аттестации объектов информатизации требованиям по безопасности информации. | ; |
| .2. 3 | |
| 8.Основные виды и особенности информации, её источников и носителей. | ; |
| .2. 4 | |
| 9.организационные меры поддержания информационной безопасности | ; |
| .2. 5 | |
| 10.О возможных угрозах безопасности информации и путях их ликвидации | ; |
| .2. 6 | |
| 11.О видах защищаемой информации (государственная тайна, конфиденциальная информация) и органах её защиты | ; |
| .2. 7 | |
| 12.Государственная тайна, как особого вида защищаемой информации по законодательству РФ. | ; |
| .2. 8 | |
| 13.Требования и политика обеспечения информационной безопасности | ; |
| .2. 9 | |
| 14.проблемы защиты информации | ; |
| .8. 4 | |
| 15.Методы защиты интеллектуальной собственности | ; |
| .8. 5 | |
| 16.законодательство в области обеспечения информационной безопасности | ; |

3.

3.1

| | | | |
|------------|---|---|---------------|
| | , | . | |
| : 7 | | | |
| : | | | |
| 1. | 0 | 4 | 16 |
| 2. | 0 | 2 | 11, 16, 8 |
| : | | | |
| 3. | 0 | 2 | 12, 16 |
| 4. | 0 | 4 | 1, 11, 12, 13 |
| : | | | |

| | | | |
|-----|---|---|-------------|
| 5. | 0 | 4 | 1, 13, 9 |
| 6. | 0 | 2 | 5, 6, 9 |
| 7. | 0 | 4 | 11, 15, 16 |
| 8. | 0 | 2 | 14, 15, 16 |
| 9. | 0 | 2 | 10, 2, 4, 6 |
| : | | | |
| 10. | 0 | 2 | 16, 3, 6 |
| 11. | 0 | 2 | 10, 6 |
| : | | | |
| 12. | 0 | 2 | 4, 9 |
| : | | | |
| 13. | - | 2 | 2, 3 |
| 14. | 0 | 2 | 2, 3 |

3.2

| | | | | |
|----|-------------------------|---|---|--------------|
| | | | | |
| :7 | | | | |
| : | | | | |
| 1. | () (), () , | 4 | 8 | 11, 12, 4, 7 |
| 2. | (). | 4 | 8 | 4, 7, 9 |

| | | | | | |
|----|-----------------|---|---|----------------|--|
| 3. | - (,). | 4 | 8 | 11, 13, 4, 7 | |
| : | | | | | |
| 4. | | 2 | 6 | 13, 4, 6, 9 | |
| : | | | | | |
| 5. | | 4 | 6 | 1, 10, 2, 3, 6 | |

4.

| | | | | | |
|---|--|--|--|----|---|
| | | | | | |
| : 7 | | | | | |
| 1 | | | 1, 10, 11, 12, 13, 14, 15, 16, 2, 3, 4, 5, 6, 8, 9 | 18 | 3 |
| <p>Internet , 3 : . . . []: - / . . ; . . - . - , [2016]. - : http://elibrary.nstu.ru/source?bib_id=vtls000233294. - .</p> | | | | | |
| 2 | | | 10, 4, 7 | 10 | 0 |
| <p>- , 1 : . . . []: - / . . ; . . - . - , [2016]. - : http://elibrary.nstu.ru/source?bib_id=vtls000233294. - .</p> | | | | | |
| 3 | | | 1, 10, 11, 12, 13, 14, 15, 16, 2, 3, 4, 5, 6, 8, 9 | 10 | 2 |
| <p>3 : . . . []: - / . . ; . . - . - , [2016]. - : http://elibrary.nstu.ru/source?bib_id=vtls000233294. - .</p> | | | | | |
| 4 | | | 1, 10, 11, 12, 13, 14, 15, 16, 2, 3, 4, 6, 7, 8, 9 | 25 | 2 |

[2 :]: - / ;
 , [2016]. - : http://elibrary.nstu.ru/source?bib_id=vtls000233294.

5.

(. 5.1).

5.1

| | |
|--|-----------------------------|
| | - |
| | e-mail:sankov@corp.nstu.ru |
| | e-mail:sankov@corp.nstu.ru |
| | e-mail:sankov@corp.nstu.ru; |
| | ; |

5.2

| | | |
|---|--|-----|
| | | |
| 1 | | .2; |
| <p>Формируемые умения: з11. методы защиты информации от утечки по техническим каналам; з12. технологические меры поддержания информационной безопасности объектов; з14. меры уменьшения ущерба от утраты информации; з2. способен соблюдать основные требования информационной безопасности; з4. организационные меры поддержания информационной безопасности; з5. возможные угрозы безопасности информации; з8. принципы и виды политики безопасности</p> | | |
| <p>Краткое описание применения: Получение практических навыков по определению и установлению организационнотехнических требований защиты секретной и конфиденциальной информации</p> | | |

6.

(),

15-

ECTS.

. 6.1.

6.1

| | | |
|---|----|----|
| | | |
| : 7 | | |
| <i>Лекция: посещение</i> | 6 | 18 |
| " / , [2016]. - [:]: http://elibrary.nstu.ru/source?bib_id=vtls000233294 . " | | |
| <i>Лабораторная №2: выполнение</i> | 10 | 10 |
| " / , [2016]. - [:]: http://elibrary.nstu.ru/source?bib_id=vtls000233294 . " | | |

| | | |
|---|----|----|
| Лабораторная №2: защита | 10 | 35 |
| " / , [2016]. - []: http://elibrary.nstu.ru/source?bib_id=vtls000233294 - " | | |
| РГЗ: выполнение и защита | 4 | 17 |
| " / , [2016]. - []: http://elibrary.nstu.ru/source?bib_id=vtls000233294 - " | | |
| Зачет: | 10 | 20 |
|] : () " / , [2016]. - []: http://elibrary.nstu.ru/source?bib_id=vtls000233294 - " | | |

6.2

6.2

| | | / | | |
|----|-----|---|---|---|
| .8 | 4. | | + | + |
| | 5. | | + | + |
| .2 | 10. | + | + | + |
| | 11. | + | + | + |
| | 12. | + | + | + |
| | 13. | | + | + |
| | 14. | + | + | + |
| | 2. | + | | |
| | 3. | | + | + |
| | 4. | + | + | |
| | 5. | + | + | + |
| | 6. | + | + | + |
| | 7. | + | + | + |
| | 8. | + | | + |
| | 9. | | + | |

1

7.

1. Романов О. А. Организационное обеспечение информационной безопасности : [учебник для вузов по специальностям "Организация и технология защиты информации" и "Комплексная защита объектов информации" направления подготовки "Информационная безопасность"] / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М., 2008. - 188, [1] с.

2. Проскурин В. Г. Защита программ и данных : [учебное пособие для вузов по специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем"] / В. Г. Проскурин. - М., 2011. - 198, [1] с.
3. Громов Ю. Ю. Информационная безопасность : учеб / Ю. Ю. Громов. - Москва, 2014
4. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6, 500 экз. - Режим доступа: <http://znanium.com/catalog.php?bookinfo=474838> - Загл. с экрана.
5. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.: 60x90 1/16. - (Высшее образование) (Переплёт) ISBN 978-5-369-01450-9 - Режим доступа: <http://znanium.com/catalog.php?bookinfo=495249> - Загл. с экрана.

1. Садердинов А. А. Информационная безопасность предприятия : учебное пособие / Садердинов А. А. , Трайнёв В. А. , Федулов А.А. ; Междунар. акад. наук информации, информ. процессов и технологий МАН ИПТ). - М., 2006. - 335 с. : ил., схемы
2. Расторгуев С. П. Основы информационной безопасности : [учебное пособие для вузов по специальностям "Компьютерная безопасность" [и др.] / С. П. Расторгуев. - М., 2007. - 186, [1] с. : ил.
3. Мельников В. П. Информационная безопасность и защита информации : [учебное пособие для вузов по специальности "Информационные системы и технологии"] / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М., 2011. - 330, [1] с. : ил., табл., схемы

1. ЭБС НГТУ : <http://elibrary.nstu.ru/>
2. ЭБС «Издательство Лань» : <https://e.lanbook.com/>
3. ЭБС IPRbooks : <http://www.iprbookshop.ru/>
4. ЭБС "Znanium.com" : <http://znanium.com/>
5. :

8.

8.1

1. Санков О. В. Информационная безопасность и защита государственной тайны [Электронный ресурс] : электронный учебно-методический комплекс / О. В. Санков ; Новосиб. гос. техн. ун-т. - Новосибирск, [2016]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000233294. - Загл. с экрана.

8.2

- 1 Windows
- 2 Office

9. -

| | | |
|---|-----------|---|
| | | |
| 1 | (-) , , | , |

| | | |
|---|--------------|--|
| | | |
| 1 | (Internet) | |

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра автономных информационных и управляющих систем

“УТВЕРЖДАЮ”
ДЕКАН ФЛА
д.т.н., профессор С.Д. Саленко
“ ____ ” _____ ____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность и защита государственной тайны

Образовательная программа: 17.05.01 Боеприпасы и взрыватели, специализация: Боеприпасы

1. Обобщенная структура фонда оценочных средств учебной дисциплины

Обобщенная структура фонда оценочных средств по дисциплине Информационная безопасность и защита государственной тайны приведена в Таблице 1.

Таблица 1.

| Формируемые компетенции | Показатели сформированности компетенций (знания, умения, навыки) | Темы | Этапы оценки компетенций | |
|---|--|---|---|---|
| | | | Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.) | Промежуточная аттестация (экзамен, зачет) |
| ОК.8 способность использовать общеправовые знания в различных сферах деятельности | 34. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты | Защита интеллектуальной собственности Коммерческая тайна | РГЗ (реферат): основная часть, заключение | Зачет, вопросы 30-34, 46-48 |
| ОК.8 | 35. вопросы правового регулирования обеспечения информационной безопасности | Введение. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации Государственная тайна как особый вид защищаемой информации Защита интеллектуальной собственности Коммерческая тайна Понятие и виды защищаемой информации по законодательству РФ Правовые аспекты применения технических средств получения и защиты информации | РГЗ (реферат): основная часть, заключение | Зачет, вопросы 1-34, 45-47 |
| ОПК.2 способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасность и угрозы возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны | 32. способен соблюдать основные требования информационной безопасности | Получение практических навыков по категорированию объектов вычислительной техники (ВТ) и выделенных помещений (ВП), предназначенных для обработки (обсуждения) секретной информации, а также классификации автоматизированных систем (АС), предназначенных для обработки секретной и конфиденциальной информации. Получение практических навыков по определению и установлению организационно-технических требований защиты секретной и конфиденциальной информации при её обработке в автоматизированной системе (АС). | Отчет по лабораторной работе №1,2,3 | |
| ОПК.2 | 33. знать сущность и значение информации в развитии | Понятие и виды защищаемой информации по законодательству РФ | РГЗ (реферат): основная часть, заключение | Зачет, вопросы 1-23 |

| | | | | |
|-------|--|--|--|----------------------|
| | современного общества, опасности и угроз, возникающие в этом процессе | | | |
| ОПК.2 | 34. организационные меры поддержания информационной безопасности | Анализ и оценка угроз информационной безопасности объекта Организация и обеспечение режима секретности Получение практических навыков по определению и установлению организационно-технических требований защиты секретной и конфиденциальной информации при её обработке в автоматизированной системе (АС). Получение практических навыков по составлению технологического процесса обработки защищаемой информации в автоматизированной системе Правовое регулирование взаимоотношений администрации и персонала в области защиты информации | Отчет по лабораторной работе №4, РГЗ (реферат): основная часть, заключение | Зачет, вопросы 37-40 |
| ОПК.2 | 35. возможные угрозы безопасности информации | Концептуальное проектирование системы физической защиты Основные методы защиты информации техническими средствами Технологические меры поддержания информационной безопасности объектов | Отчет по лабораторной работе №5, РГЗ (реферат): основная часть, заключение | Зачет, вопросы 43,44 |
| ОПК.2 | 36. виды защищаемой информации | Коммерческая тайна Получение практических навыков по категорированию объектов вычислительной техники (ВТ) и выделенных помещений (ВП), предназначенных для обработки (обсуждения) секретной информации, а также классификации автоматизированных систем (АС), предназначенных для обработки секретной и конфиденциальной информации. Понятие и виды защищаемой информации по законодательству РФ Система защиты государственной тайны | Отчет по лабораторной работе №1, 2, 3. РГЗ (реферат): основная часть, заключение | Зачет, вопросы 4-29 |
| ОПК.2 | 37. требования по защите государственной и коммерческой тайны на предприятиях оборонно-промышленного комплекса | Государственная тайна как особый вид защищаемой информации Получение практических навыков по категорированию объектов вычислительной техники (ВТ) и выделенных помещений (ВП), предназначенных для обработки (обсуждения) | Отчет по лабораторной работе №1, 2, 3. РГЗ (реферат): основная часть, заключение | Зачет, вопросы 24-29 |

| | | | | |
|-------|--|---|---|--------------------------|
| | | секретной информации, а также классификации автоматизированных систем (АС), предназначенных для обработки секретной и конфиденциальной информации. Система защиты государственной тайны | | |
| ОПК.2 | 38. принципы и виды политики безопасности | Организация и обеспечение режима секретности Получение практических навыков по определению и установлению организационно-технических требований защиты секретной и конфиденциальной речевой информации при её обсуждении в выделенном либо защищаемом помещении (ВП, ЗП). Получение практических навыков по составлению технологического процесса обработки защищаемой информации в автоматизированной системе Система защиты государственной тайны | Отчет по лабораторной работе №3, 4. | Зачет, вопросы 35,36,42 |
| ОПК.2 | 39. проблемы защиты информации | Защита интеллектуальной собственности | РГЗ (реферат): основная часть, заключение | |
| ОПК.2 | 310. способы и методы комплексной защиты информации | Концептуальное проектирование системы физической защиты Организация и обеспечение режима секретности Система защиты государственной тайны | Отчет по лабораторной работе №5, РГЗ (реферат): основная часть, заключение | Зачет, вопросы 35,36,42 |
| ОПК.2 | 311. методы защиты информации от утечки по техническим каналам | Концептуальное проектирование системы физической защиты Правовые аспекты применения технических средств получения и защиты информации Принципы инженерно-технической защиты информации Средства и методы физической защиты объектов Технологические меры поддержания информационной безопасности объектов | Отчет по лабораторной работе №5 РГЗ (реферат): основная часть, заключение | Зачет, вопросы 41, 52-55 |
| ОПК.2 | 312. технологические меры поддержания информационной безопасности объектов | Анализ и оценка угроз информационной безопасности объекта Получение практических навыков по категорированию объектов вычислительной техники (ВТ) и выделенных помещений (ВП), предназначенных для обработки (обсуждения) секретной информации, а также классификации автоматизированных систем (АС), предназначенных для | Отчет по лабораторной работе №1, 2, 3, 4 РГЗ (реферат): основная часть, заключение | Зачет, вопросы 48-51 |

| | | | | |
|-------|--|--|---|----------------------|
| | | <p>обработки секретной и конфиденциальной информации. Получение практических навыков по определению и установлению организационно-технических требований защиты секретной и конфиденциальной информации при её обработке в автоматизированной системе (АС). Получение практических навыков по определению и установлению организационно-технических требований защиты секретной и конфиденциальной речевой информации при её обсуждении в выделенном либо защищаемом помещении (ВП, ЗП). Получение практических навыков по составлению технологического процесса обработки защищаемой информации в автоматизированной системе</p> <p>Технологические меры поддержания информационной безопасности объектов</p> | | |
| ОПК.2 | з13. обязанности руководства объекта и персонала при работе с защищаемой информацией | <p>Правовое регулирование взаимоотношений администрации и персонала в области защиты информации</p> | РГЗ (реферат): основная часть, заключение | Зачет, вопросы 37-39 |
| ОПК.2 | з14. меры уменьшения ущерба от утраты информации | <p>Концептуальное проектирование системы физической защиты Основные методы защиты информации техническими средствами</p> <p>Получение практических навыков по составлению технологического процесса обработки защищаемой информации в автоматизированной системе</p> <p>Правовое регулирование взаимоотношений администрации и персонала в области защиты информации</p> <p>Правовые аспекты применения технических средств получения и защиты информации</p> <p>Технологические меры поддержания информационной безопасности объектов</p> | <p>Отчет по лабораторной работе №5</p> <p>РГЗ (реферат): основная часть, заключение</p> | Зачет, вопросы 37-40 |

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 7 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций

ОК.8, ОПК.2.

Зачет проводится в письменной форме, по билетам, варианты которых составляются из вопросов, приведенных в паспорте зачета, позволяющих оценить показатели сформированности соответствующих компетенций

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 7 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе учебной дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОК.8, ОПК.2, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра автономных информационных и управляющих систем

Паспорт зачета

по дисциплине «Информационная безопасность и защита государственной тайны», 7
семестр

1. Методика оценки

Зачет проводится в письменной форме по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-35, второй вопрос из диапазона вопросов 36-55 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет ФЛА

Билет № _____

к зачету по дисциплине «Информационная безопасность и защита государственной
тайны»

1. Вопрос 1
2. Вопрос 2.

Утверждаю: зав. кафедрой _____ должность, ФИО
(подпись)

(дата)

Пример билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет ФЛА

Билет № 4

к зачету по дисциплине «Информационная безопасность и защита государственной тайны»

Вопрос 1) Отличительные признаки защищаемой информации

Вопрос 2) Анализ и оценка угроз информационной безопасности объекта

Утверждаю: зав. кафедрой АИУС _____ Легкий В.Н.
(подпись) (дата)

2. Критерии оценки

- Ответ на билет для зачета считается неудовлетворительным, если даны неверные ответы на вопросы, или ответы отсутствуют, оценка составляет 0-4 баллов.
- Ответ на билет (тест) для зачета засчитывается на **пороговом** уровне, если даны неточные ответы на вопросы, оценка составляет 5 баллов за вопрос и 10 баллов за работу.
- Ответ на билет (тест) для зачета билет засчитывается на **базовом** уровне, если даны неполные ответы на вопросы, оценка составляет 6 - 9 баллов за вопрос и 12-18 баллов за работу в зависимости от полноты ответов.
- Ответ на билет (тест) для зачета билет засчитывается на **продвинутом** уровне, если даны правильные и полные ответы на вопросы, оценка составляет 10 баллов за вопрос и 20 баллов за работу.

3. Шкала оценки

Оценка знаний и умений студентов проводится с помощью вопросов по основным проблемам дисциплины. Для оценки деятельности студента используются зачетные задания в виде **2-х теоретических вопросов**. Теоретические вопросы формулируются в строгом соответствии с темами лекционных занятий. Максимальное количество баллов, которое студент может получить на зачете, равно **20**.

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее 10 баллов (из 20 возможных). Устанавливаются следующие правила аттестации студента (таблица 1).

Таблица 1

| Характер ответа | Количество баллов за ответ |
|----------------------------|----------------------------|
| Правильный ответ на вопрос | 10 |
| Неполный ответ на вопрос | 6 - 9 |
| Неточный ответ на вопрос | 5 |

В общей оценке по дисциплине баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Вопросы к зачету по дисциплине «Информационная безопасность и защита государственной тайны»

1. Информационная безопасность
2. Аспекты информационной безопасности
3. Уровни формирования режима информационной безопасности
4. Основные задачи в сфере обеспечения информационной безопасности, определяемым государством
5. Информационная сфера
6. Информационное законодательство
7. Законодательство в информационной сфере
8. Законодательство в области обеспечения информационной безопасности
9. Концепция национальной безопасности Российской Федерации
10. Национальная безопасность Российской Федерации
11. Национальные интересы России
12. Доктрина информационной безопасности Российской Федерации
13. Основные составляющие национальных интересов Российской Федерации в информационной сфере
14. Основные объекты информационной безопасности государства
15. Собственник защищаемой информации
16. Владелец защищаемой информации
17. Три группы информационных ресурсов государства
18. Отличительные признаки защищаемой информации
19. Классификация информации по степени ее секретности
20. Владельцы (собственники) защищаемой информации
21. Носители информации
22. Классификация носителей защищаемой информации
23. Документ Изделия (предметы) как носители защищаемой информации
24. Определение понятия «Государственная тайна»
25. Какие сведения следует относить
 - к сведениям особой важности
 - к совершенно секретным сведениям
 - к секретным сведениям
26. Какую информацию нельзя засекречивать
27. Политический ущерб
28. Экономический ущерб
29. Моральный ущерб
30. Определение понятия «Коммерческая тайна»
31. Какая информация составляет коммерческую тайну предприятия
32. Объекты интеллектуальной собственности
33. Сведения, которые не могут составлять коммерческую тайну
34. Степени секретности коммерческой тайны (перечислить)

35. Требования обеспечения безопасности
36. Задачи, которые решает комплексная защита КИ
37. Работа с персоналом
38. Политика безопасности и процедуры внутрифирменной коммуникации
39. Сервисы безопасности
40. Правовые аспекты применения технических средств получения и защиты информации
41. Принципы инженерно-технической защиты информации
42. Организационная защита
43. Технические мероприятия
44. Основные методы защиты информации техническими средствами
45. Защита интеллектуальной собственности
46. Объект авторского права.
47. Товарный знак
48. Анализ и оценка угроз информационной безопасности объекта
49. Анализ информационных рисков
50. Аудит информационной безопасности
51. Работы по аудиту безопасности ИС
52. Система физической защиты, комплексная система безопасности
53. Процесс создания (модернизации) СФЗ, КСБ. Концептуальное проектирование СФЗ,
54. Пути построения и модернизации СФЗ. Проблемы построения СФЗ
55. Оценка эффективности СФЗ

Паспорт расчетно-графического задания (работы)

по дисциплине «Информационная безопасность и защита государственной тайны», 7
семестр

1. Методика оценки

Изложение темы работы построить на "свободных" примерах, которые позволили бы достаточно объективно оценить уровень подготовки и правильность понимания существа рассматриваемой в данной теме проблемы. Должны быть также представлены определения понятий, используемых по ходу изложения.

Требования к оформлению работы:

1. Работа выполняется в печатном виде на бумаге формата А4, размер шрифта 14, интервал 1.5, объемом 10-15 страниц.
2. Оформляется титульный лист;
3. Оформляется содержание работы
4. На нескольких страницах кратко рассматриваются вопросы, регулирующие соответствующую тему;
5. После рассмотрения всех запланированных вопросов, подводятся выводы по поводу рассмотренной темы.
6. Приводится список используемых литературных источников.

Обязательные структурные части РГЗ (реферата).

- Введение (актуальность темы, рассматриваемые вопросы, цель работы).
- Основная часть.
- Заключение (выводы по работе, полученные результаты).
- Список используемых литературных источников

Оцениваемые позиции:

- Соответствие оформления работы требованиям.
- Наличие обязательных разделов.
- Содержание основной части работы.
- Презентация работы при защите.
- Ответы студента при защите работы.

2. Критерии оценки

- Работа считается не выполненной, если выполнены не все части РГЗ (Реферат), уровень выполнения не отвечает требованиям, студент при защите не отвечает на вопросы по теме задания, оценка составляет **0-3** баллов.
- Работа считается выполненной на пороговом уровне, если работа слабая, уровень выполнения не отвечает большинству требований, студент при защите отвечает

мене чем на половину вопросов по теме задания, оценка составляет **4-9** баллов, в зависимости от числа правильных ответов при защите.

- Работа считается выполненной на базовом уровне, если уровень выполнения отвечает большинству требований, студент при защите отвечает на большинство вопросов по теме задания, оценка составляет **10-14** баллов, в зависимости от числа правильных ответов при защите.
- Работа считается выполненной на продвинутом уровне, если работа высокого качества, уровень выполнения отвечает всем требованиям, студент при защите отвечает на все вопросы по теме задания, оценка составляет **15-17** баллов.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ (реферат) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

Для допуска к зачету необходимо защитить РГЗ (реферат). Оценка за РГЗ составляет от 6 до 15 баллов из 80 возможных в рамках текущей аттестации в семестре.

4. Примерный перечень тем РГЗ(Р)

- 1.** Методы защиты информации
- 2.** Государственная тайна
- 3.** Коммерческая тайна
- 4.** Аудит информационной безопасности
- 5.** Виды защищаемой информации
- 6.** Законодательство в области защиты информации
- 7.** Правовое регулирование применения средств защиты информации
- 8.** Защита интеллектуальной собственности