МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФГБОУ ВО «Брянский государственный технический университет»

Факультет информационных технологий

Кафедра «Системы информационной безопасности»

УТВЕРЖДАЮ
Председатель приемной комиссии,
ректор БГТУ
_____ О.Н. Федонин
«03» июня 2021 г.

ПРОГРАММА
вступительного испытания
для поступающих на направление подготовки
10.06.01- Информационная безопасность,
направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

Брянск 2021

Программа вступительного испытания для поступающих на направление подготовки 10.06.01 - Информационная безопасность, направленность (профиль): «Методы и системы защиты информации, информационная безопасность».

Разработал:
Заведующий кафедрой
«Системы информационной безопасности»
канд. тех. наук, доцент _____ Рытов М.Ю.

Программа вступительного испытания рассмотрена и одобрена на заседании кафедры «Системы информационной безопасности»: протокол №10 от «14» мая 2021г.

Заведующий кафедрой
канд. тех. наук, доцент _____ / Рытов М.Ю. /

Проректор по научной работе
к.т.н., доцент _____ /Сканцев В.М./

1. ОБЩИЕ ПОЛОЖЕНИЯ

Вступительное испытание при приеме в аспирантуру по направлению 10.06.01 - Информационная безопасность, направленность (профиль) «Методы и системы защиты информации, информационная безопасность» (далее - аспирантура) проводится ФГБОУ ВО «Брянский государственный технический университет» (далее – Университет, вуз, БГТУ) самостоятельно.

Программа вступительного испытания сформирована на основе федеральных государственных образовательных стандартов высшего образования по программам специалитета или магистратуры.

Вступительное испытание при приеме в аспирантуру проводится на государственном языке Российской Федерации в письменной или устно-письменной форме.

Вступительные испытания могут проводиться: 1) при личном присутствии в Университете претендента на обучение в аспирантуру (контактный формат); 2) при отсутствии в Университете претендента на обучение в аспирантуру (дистанционный формат).

При контактном формате проведения вступительного испытания претендент лично присутствует на вступительном испытании, которое проводится в Университете в заранее определенной аудитории.

При невозможности присутствия в Университете претендента на обучение в аспирантуру вступительное испытание полностью проводится с применением электронного обучения, дистанционных образовательных технологий (дистанционный формат).

Проведение вступительного испытания в дистанционном формате допускается в следующих случаях:

- при возникновении у абитуриента исключительных обстоятельств (уважительных причин), препятствующих его личному присутствию в Университете для прохождения вступительных испытаний;

- при нормативно-правовом установлении особого режима работы Университета, не допускающего личное присутствие абитуриентов в Университете.

К исключительным обстоятельствам, препятствующим абитуриенту лично присутствовать в Университете при прохождении вступительных испытаний, относится, при наличии подтверждающих документов, состояние здоровья для абитуриентов-инвалидов и абитуриентов с ограниченными возможностями здоровья.

Нормативно-правовое установление особого режима работы Университета, обусловленное чрезвычайной ситуацией или режимом повышенной готовности

техногенного, биологического, экологического или иного характера, регулируется нормативно-правовым актом учредителя Университета или высшего должностного лица субъекта Российской Федерации и делает невозможным контактный формат проведения вступительного испытания в Университет.

Решение о формате прохождения абитуриентом вступительного испытания принимает приемная комиссия Университета.

При нормативно-правовом установлении особого режима работы Университета, не допускающего личное присутствие абитуриентов в Университете при прохождении вступительного испытания, решение о проведении вступительного испытания с применением электронного обучения, дистанционных образовательных технологий (в дистанционном формате) принимается единообразно для всех абитуриентов.

Формат проведения вступительного испытания доводится до сведения абитуриента заблаговременно.

При проведении вступительного испытания Университетом могут использоваться следующие дистанционные технологии: электронная информационно-образовательная среда вуза, видеоконференцсвязь, электронная почта, компьютерное тестирование.

2. ПРОВЕДЕНИЕ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ В КОНТАКТНОМ ФОРМАТЕ

Длительность проведения вступительного испытания в контактном формате - 3 астрономических часа (180 минут).

Экзаменационный билет содержит 3 вопроса. Перечень вопросов, содержащихся в экзаменационных билетах, представлен в п. 4 настоящей программы.

За отведенное время абитуриент должен представить письменные развернутые ответы на каждый вопрос экзаменационного билета. Ответы абитуриент записывает на бланке приемной комиссии Университета, который он получает вместе с экзаменационным билетом.

Результаты вступительного испытания оцениваются по стобальной шкале (100 баллов).

За ответы на вопросы экзаменационного билета может быть начислено:

- за ответ на первый вопрос билета (вопросы №1…25 из п. 4 настоящей программы) – до 50 баллов;

- за ответ на второй вопрос билета (вопросы №26…50 из п. 4 настоящей программы) – до 30 баллов;

- за ответ на третий вопрос билета (вопросы №51…75 из п. 4 настоящей программы) – до 20 баллов;

Применяются критерии оценки знаний, представленные в таблице 1.

Методика выставления оценки базируется на совокупной оценке всех членов экзаменационной комиссии, сформированной на основе независимых оценок каждого члена комиссии. Итоговая оценка абитуриента за вступительное испытание рассчитывается как сумма полученных баллов за ответы на все вопросы экзаменационного билета.

Минимальная положительная оценка для аттестации по вступительному испытанию - 41 балл, максимальная оценка – 100 баллов.

После проверки результатов вступительного испытания комиссия может провести индивидуальное собеседование с абитуриентом для уточнения отдельных положений в рамках вопросов билета.

Обнаружение у абитуриента несанкционированных экзаменационной комиссией учебных и методических материалов, пользование любыми средствами передачи информации (электронными средствами связи) является основанием для принятия решения о выставлении оценки «неудовлетворительно» по результатам вступительного испытания («0» по 100-балльной шкале), вне зависимости от того, были ли использованы указанные материалы (средства) при подготовке ответа.

Таблица 1 - Критерии оценивания знаний абитуриента при проведении вступительного испытания

Оценка (баллы)	Критерии оценивания
Вопрос 1	
44-50	- высокий уровень осведомленности по теме; - ответы на вопросы демонстрируют свободное владение абитуриентом материалом в рамках обозначенной темы на 90 – 100 %; - на 90 – 100 % продемонстрирована способность анализировать и систематизировать теоретический материал, умение обрабатывать информацию междисциплинарного характера и устанавливать причинно-следственные связи.
33-43	- средний уровень осведомленности по теме; - ответы на вопросы демонстрируют владение абитуриентом теоретическим материалом по изучаемым разделам дисциплины на 70–89%; - на 70 – 89% продемонстрирована способность анализировать и систематизировать теоретический материал, умение обрабатывать информацию междисциплинарного характера и устанавливать причинно-следственные связи.
22-32	- низкий уровень осведомленности по теме;

Оценка (баллы)	Критерии оценивания
	- ответы на вопросы выявляют владение абитуриентом теоретическим материалом на 50 – 69 %; - на 50 – 69 % продемонстрирована способность анализировать и систематизировать теоретический материал; - отсутствие у абитуриента минимального объема знаний по ранее изученным и смежным дисциплинам и, как следствие, слабовыраженные способности к выявлению причинно-следственных связей.
0-21	- неудовлетворительный уровень осведомленности по теме; - ответы на вопросы характеризуют владение абитуриентом теоретическим материалом менее, чем на 50%; - ответы на вопросы свидетельствуют об отсутствии у абитуриента осведомленности по теме; - отсутствие у абитуриента способности анализировать и систематизировать теоретический материал, умения обрабатывать информацию междисциплинарного характера и устанавливать причинно-следственные связи.
Вопрос 2	
25-30	- высокий уровень осведомленности по теме; - ответы на вопросы демонстрируют свободное владение абитуриентом материалом в рамках обозначенной темы на 90 – 100%; - на 90 – 100% продемонстрирована способность анализировать и систематизировать теоретический материал, умение обрабатывать информацию междисциплинарного характера и устанавливать причинно-следственные связи.
18-24	- средний уровень осведомленности по теме; - ответы на вопросы демонстрируют владение абитуриентом теоретическим материалом по изучаемым разделам дисциплины на 70 – 89 %; - на 70 – 89 % продемонстрирована способность анализировать и систематизировать теоретический материал, умение обрабатывать информацию междисциплинарного характера и устанавливать причинно-следственные связи.
11-17	- низкий уровень осведомленности по теме; - ответы на вопросы выявляют владение абитуриентом теоретическим материалом на 50 – 69 %; - на 50 – 69 % продемонстрирована способность анализировать и систематизировать теоретический материал; - отсутствие у абитуриента минимального объема знаний по ранее изученным и смежным дисциплинам и, как следствие, слабовыраженные способности к выявлению причинно-следственных связей.
0-10	- неудовлетворительный уровень осведомленности по теме;

Оценка (баллы)	Критерии оценивания
	- ответы на вопросы характеризуют владение абитуриентом теоретическим материалом менее, чем на 50%; - ответы на вопросы свидетельствуют об отсутствии у абитуриентов осведомленности по теме; - отсутствие у абитуриента способности анализировать и систематизировать теоретический материал, умения обрабатывать информацию междисциплинарного характера и устанавливать причинно-следственные связи.
Вопрос 3	
17-20	- высокий уровень осведомленности по теме; - ответы на вопросы демонстрируют свободное владение абитуриентом материалом в рамках обозначенной темы на 90 – 100 %; - на 90 – 100 % продемонстрирована способность анализировать и систематизировать теоретический материал, умение обрабатывать информацию междисциплинарного характера и устанавливать причинно-следственные связи.
13-16	- средний уровень осведомленности по теме; - ответы на вопросы демонстрируют владение абитуриентом теоретическим материалом по изучаемым разделам дисциплины на 70 – 89 %; - на 70 – 89 % продемонстрирована способность анализировать и систематизировать теоретический материал, умение обрабатывать информацию междисциплинарного характера и устанавливать причинно-следственные связи.
8-12	- низкий уровень осведомленности по теме; - ответы на вопросы выявляют владение абитуриентом теоретическим материалом на 50 – 69 %; - на 50 – 69 % продемонстрирована способность анализировать и систематизировать теоретический материал; - отсутствие у абитуриента минимального объема знаний по ранее изученным и смежным дисциплинам и, как следствие, слабовыраженные способности к выявлению причинно-следственных связей.
0-7	- неудовлетворительный уровень осведомленности по теме; - ответы на вопросы характеризуют владение абитуриентом теоретическим материалом менее, чем на 50%; - ответы на вопросы свидетельствуют об отсутствии у абитуриента осведомленности по теме; - отсутствие у абитуриента способности анализировать и систематизировать теоретический материал, умения обрабатывать информацию междисциплинарного характера и устанавливать причинно-следственные связи.

3. ПРОВЕДЕНИЕ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ В ДИСТАНЦИОННОМ ФОРМАТЕ

Вступительное испытание в дистанционном формате, как правило, проводится в виде компьютерного тестирования с использованием технологии видеоконференцсвязи для идентификации личности абитуриента в электронной информационно-образовательной среде (ЭИОС) БГТУ. Доступ к ресурсам и технологиям ЭИОС БГТУ осуществляется абитуриентом через информационно-телекоммуникационную сеть Интернет.

Длительность проведения вступительного испытания в дистанционном формате определяется заранее и фиксируется в ЭИОС БГТУ.

Результаты вступительного испытания оцениваются по стобальной шкале (100 баллов), т.е. максимальная оценка – 100 баллов.

Компьютерный тест содержит фиксированное количество вопросов.

Правильное выполнение каждого тестового задания оценивается определенным количеством баллов. При неполном (частичном) выполнении тестового задания сумма баллов за него пропорционально уменьшается с математическим округлением до целого числа баллов. При неправильном выполнении или невыполнении тестового задания, баллы за него не начисляются.

Общая сумма набранных баллов за правильные ответы является балльной оценкой результата сдачи абитуриентом вступительного испытания.

Основные параметры компьютерного теста, применяемого для аттестации абитуриента по вступительному испытанию для поступления в аспирантуру, приведены в таблице 2.

Набор тестовых заданий формируется индивидуально для каждого абитуриента в ЭИОС Университета автоматически. При этом, по каждому вопросу из перечня вопросов, выносимых на вступительные испытания (см п. 4 программы) может содержаться несколько тестовых заданий различных видов (см п. 6 программы).

Таблица 2 – Параметры компьютерного теста, применяемого для аттестации абитуриента по вступительному испытанию для поступления в аспирантуру по направлению 10.06.01 - Информационная безопасность, направленность (профиль) «Методы и системы защиты информации, информационная безопасность»

№ п/п	Наименование параметра	Значение параметра	Единицы измерения
1.	Количество вопросов (тестовых заданий) в тесте	25	штуки
2.	Минимальное количество баллов	41	баллы

	для аттестации по вступительному испытанию		
3.	Максимальное количество баллов	100	баллы
4.	Время, отведенное на прохождение теста	60	минуты

Вступительное испытание в форме компьютерного тестирования проводится с применением технологии видеоконференции в режиме реального времени и может быть записано техническими средствами Университета.

Информация о проведении вступительного испытания с применением электронного обучения, дистанционных образовательных технологий, а также о дате, времени и способе выхода на связь для его прохождения доводится до абитуриента путем размещения информации в личном кабинете абитуриента, а также, в случае необходимости, по другим доступным каналам связи (посредством передачи по электронной почте, СМС-уведомлением, путем объявления на официальном сайте вуза в сети Интернет и др.).

Абитуриент самостоятельно технически оснащает и настраивает свое индивидуальное автоматизированное рабочее место, которое должно содержать следующие технические средства:

- персональный компьютер, подключенный к информационно-коммуникационной сети Интернет;
- web-камеру, подключенную к персональному компьютеру и направленную на абитуриента, обеспечивающую передачу видеоизображения или аудиовидеоинформации;
- комплект акустического оборудования (микрофон и звуковые колонки или только звуковые колонки в случае передачи web-камерой аудиоинформации), обеспечивающего обмен аудиоинформацией между абитуриентом и членами приемной комиссии Университета.

Доступ к ЭИОС Университета абитуриент получает после подачи заявления о приеме с приложением необходимых документов в приемную комиссию Университета и допуска к прохождению вступительных испытаний.

Университет, при необходимости, силами работников приемной комиссии оказывает консультационную поддержку абитуриента по техническим вопросам подключения индивидуального автоматизированного рабочего места абитуриента к ЭИОС Университета.

Университет, в процессе проведения компьютерного тестирования, может применять систему мониторинга процесса прохождения вступительных испытаний абитуриентом (прокторинга). В случае применения Университетом

системы прокторинга абитуриент информируется об этом до начала прохождения процедуры сдачи вступительного испытания.

Аудиовидеозапись процедуры прохождения абитуриентом вступительного испытания является материалом для служебного пользования, оглашение которого возможно только по письменному разрешению председателя приемной комиссии Университета, в том числе, в случае подачи абитуриентом апелляции.

Аудиовидеозапись процедуры прохождения абитуриентом вступительного испытания наряду с результатами компьютерного тестирования, рассматривается Приемной комиссией Университета при вынесении решения о результатах сдачи абитуриентом вступительного испытания и/или апелляционной комиссией Университета в случае подачи абитуриентом апелляции.

Процедуре прохождения абитуриентом компьютерного тестирования предшествует процедура идентификации его личности, которая осуществляется путем демонстрации абитуриентом на web-камеру разворота документа, удостоверяющего его личность и содержащего фотографию, фамилию, имя, отчество (при наличии) абитуриента и позволяющего четко сличить фотографию на документе с транслируемым видеоизображением абитуриента.

Если абитуриент отказался подтвердить согласие с правилами прохождения вступительных испытаний и/или согласие на обработку персональных данных и/или не прошел процедуру идентификации личности, дальнейшие действия абитуриента по прохождению вступительного испытания невозможны, вступительное испытание считается не начатым, а по истечении сроков его прохождения – не пройденным (0 баллов).

При прохождении компьютерного тестирования, абитуриент **обязан**:

- не передавать реквизиты доступа к своей учетной записи в ЭИОС Университета третьим лицам;

- обеспечить необходимые условия для работы индивидуального автоматизированного рабочего места, в том числе достаточный уровень освещенности, низкий уровень шума, отсутствие помех передаче видео и аудио сигналов;

- использовать для идентификации оригинал документа, удостоверяющего его личность, с фотографией;

- не покидать зону видимости камеры в течение всего процесса тестирования;

- не отключать микрофон и не снижать его уровень чувствительности к звуку;

- использовать в составе индивидуального автоматизированного рабочего места только одно средство вывода изображения (монитор, телевизионная панель и др.), одну клавиатуру, один манипулятор (компьютерную мышь, трекпойнт и др.);

- не привлекать на помощь третьих лиц, не отвлекаться на общение с третьими лицами и не предоставлять доступ к компьютеру посторонним лицам;

- не использовать справочные материалы, представленные на различных носителях (книги, записи в бумажном и электронном видах и др.), электронные устройства, не входящие в состав автоматизированного рабочего места (мобильные телефоны, планшеты и др.), дополнительные мониторы и компьютерную технику, не открывать вкладки поисковых систем браузера (Яндекс, Google и др).

Выявление экзаменационной комиссией, в том числе, с применением системы прокторинга, нарушений абитуриентом указанных выше обязательств в процессе сдачи вступительного испытания, является основанием для принятия экзаменационной комиссией решения о снижении оценки или выставлении абитуриенту оценки «неудовлетворительно» по результатам вступительного испытания («0» по 100-балльной шкале).

4. ПЕРЕЧЕНЬ ВОПРОСОВ, ВЫНОСИМЫХ В ЭКЗАМЕНАЦИОННЫЕ БИЛЕТЫ

Модуль «Организационно-правовая защита информации»

1. Общая характеристика организационных методов защиты информации.
2. Основные принципы организации системы безопасности объекта. Модель комплексной системы безопасности.
3. Классификация угроз информационной безопасности. Виды КУИ.
4. Основные направления организационной защиты информации на объекте.
5. Каналы несанкционированного доступа к информации. Их характеристика.
6. Характеристика типовой структуры службы безопасности.
7. Основные задачи службы безопасности объекта.
8. Характеристика функций службы безопасности объекта.
9. Права, обязанности и ответственность сотрудников службы безопасности.
10. Организация режима и охраны на объекте. Основные задачи.
11. Способы пресечения разглашения защищаемой информации.
12. Организация аттестации защищенных помещений.
13. Персонал фирмы и его роль в утечке информации.
14. Основные рекомендации при организации проверки и отбора кандидатов на работу в коммерческие предприятия.
15. Особенности увольнения сотрудников, владеющих конфиденциальной информацией.
16. Защита информации при проведении совещаний и переговоров.
17. Защита информации при работе с посетителями.

18. Характеристика информационно-аналитической работы.
19. Общий подход к категорированию объектов охраны.
20. Организация защиты информации при публикаторской и рекламной деятельности.
21. Основные этапы подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.
22. Лицензирование и сертификация в области защиты информации в РФ.
23. Коммерческая тайна и порядок её определения.
24. Организация работ с информацией, составляющей коммерческую тайну.

Модуль «Техническая защита информации»

25. Виды информации, защищаемой техническими средствами.
26. Основные принципы защиты информации техническими средствами.
27. Методы защиты информации техническими средствами.
28. Понятие, классификация демаскирующих признаков
29. Технические каналы утечки информации.
30. Основной подход построения инженерно-техническая система защиты
31. Цели системы технической защиты
32. Входные данные для проектирования системы защиты
33. Алгоритм проектирования инженерно-технической системы защиты.
34. Этапы моделирования объекта защиты
35. Демаскирующие признаки каналов утечки информации.
36. Типовые средства и способы защиты информации.
37. Структура системы инженерно-технической системы защиты информации
38. Организационно-технические мероприятия, проводимые при защите информации техническими средствами
39. Основа комплекса технической защиты информации
40. Основные способы маскировки.
41. Основные способы противодействия подслушиванию.
42. Способы контроля помещения на отсутствие закладных устройств
43. Средства и методы инженерной защиты.
44. Основные способы идентификации на контрольно-пропускных пунктах.
45. Типовая структура системы охранной сигнализации
46. Классификация извещателей охранно-пожарных извещателей.
47. Назначение средств телевизионного наблюдения
48. Типовая структура системы телевизионного наблюдения
49. Порядок проектирования системы телевизионного наблюдения
50. Основные меры организационно-технической защиты информации.

Модуль «Обеспечение компьютерной безопасности»

51. История теории и практики компьютерной безопасности;
52. Структура понятия «компьютерная безопасность»;
53. Основные направления обеспечения компьютерной безопасности;
54. Принципы обеспечения компьютерной безопасности;
55. Методы и механизмы обеспечения компьютерной безопасности;

56. Понятие, классификация, оценивание угроз безопасности компьютерной информации.
57. Создания компьютерной системы с учетом обеспечения информационной безопасности;
58. Человеческий фактор и модель нарушителя безопасности информации
59. Понятие и сущность политики безопасности и модели безопасности;
60. Виды и характеристики моделей безопасности компьютерных систем;
61. Применение и показатели защищенности межсетевых экранов
62. Применение «Общих критериев» при оценке защищенных систем
63. Построение парольных систем. Угрозы безопасности парольных систем
64. Разновидности способов аутентификации

Модуль «Защита персональных данных»

65. Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных.
66. Основные положения ФЗ № 152 «О персональных данных».
67. Основные положения Постановления № 1119 «Об утверждении порядка требований к защите персональных данных при их обработке в информационных системах персональных данных».
68. Обеспечение контроля и надзора за выполнением требований по защите ПДн. Виды предусмотренных законодательством проверок.
69. Перечень нормативно-правовых актов, регламентирующих порядок наказаний за нарушение правил обработки персональных данных.
70. Типы информационных систем персональных данных
71. Порядок определения наличия недекларированных возможностей в системной и прикладном ПО
72. Определения уровня защищенности ИСПДн
73. Методика определения актуальных угроз безопасности ИСПДн.
74. Модель угроз безопасности ИСПДн. Модель нарушителя.
75. Выполнение мер по защите информационных систем персональных данных в соответствии с приказом №21 ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература:

1. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 268 с. — 978-89838-487-6. — Режим доступа: http://www.iprbookshop.ru/6991.html
2. Аверченков В.И. Криптографические методы защиты информации [Текст] + [Электронный ресурс]: учебное пособие/ В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак. – Брянск: БГТУ, 2011. – 216 с. – (Серия «Организация и технология защиты информации»)

3. Аверченков, В.И. Конкурентная разведка: технологии и противодействие: учеб. пособие / В.И. Аверченков, В.В. Спасенников, М.Ю. Рытов, Е.В. Лексиков. – Брянск: БГТУ, 2014. –200 с. 10 экз.
4. Аверченков, В.И. Методы и средства инженерно-технической защиты информации / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин, – Брянск: БГТУ, 2010. – 187 с. 53 экз
5. Гулак, М.Л. Основы компьютерной безопасности: учебное пособие/ М.Л. Гулак, М.Ю. Рытов – Брянск: БГТУ, 2013. – 216 с. 15 экз

Дополнительная литература:

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос-АРВ, 2001. – 480 с.
2. Воробьев Е.Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] : учебное пособие / Е.Г. Воробьев. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 432 c. — 978-5-4383-0120-2. — Режим доступа: http://www.iprbookshop.ru/66796.html
3. Галатенко, В.А. Стандарты информационной безопасности [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : , 2016. — 307 с. — Режим доступа: https://e.lanbook.com/book/100511. — Загл. с экрана.
4. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс] : учеб. пособие / Н.С. Кармановский, О.В. Михайличенко, Н.Н. Прохожев. — Электрон. дан. — Санкт-Петербург : НИУ ИТМО, 2016. — 168 с. — Режим доступа: https://e.lanbook.com/book/91449. — Загл. с экрана.

6. ПРИМЕРЫ ТЕСТОВЫХ ЗАДАНИЙ

6.1. Пример тестового задания с одним вариантом ответа

1. *Угрозой информационной безопасности* называется:
   A. совокупность условий и факторов, создающих опасность нарушения информационной безопасности;
   B. свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации;
   C. потенциальные возможности использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации.

2. По предложенному описанию определите тип документа: «Совокупность документированных руководящих принципов, правил,

процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации»

а) Модель угроз безопасности информации;
б) Политика информационной безопасности;
в) Инструкция администратора безопасности.

6.2. Пример тестового задания с несколькими вариантами ответов

Основными способами маскировки являются:

A. Скрытие;
B. Имитация;
C. Уничтожение;
D. Демонстративные действия;
E. Дезинформация;

6.3. Пример тестового задания на установление соответствия

Установите соответствие между термином и определением.

А) Информационная система	1) Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и производственным оборудованием и производимыми ими процессами, а также для управления такими оборудованием и процессами
Б) Компьютерный инцидент	2) Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
В) Информационно-телекоммуникационная сеть	3) Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники
Г)Автоматизированная система управления	4) Факт нарушения и прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и нарушения безопасности обрабатываемой таким объектом информации