МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

Приложение 2
к рабочей программе дисциплины

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Основы информационной безопасности

(наименование дисциплины(модуля)

Направление подготовки / специальность

09.03.03 Прикладная информатика
(код и наименование)

Направленность (профиль)/специализация

Прикладная информатика на железнодорожном транспорте
(наименование)

Содержание

1. Пояснительная записка

Цель промежуточной аттестации – оценивание промежуточных и окончательных результатов обучения по дисциплине, обеспечивающих достижение планируемых результатов освоения образовательной программы.

Перечень компетенций, формируемых в процессе освоения дисциплины

Код и наименование компетенции	Код индикатора достижения компетенции
ОПК-3.2Применяет методы защиты информации при выполнении задач профессиональной деятельности	**Знает:** методы защиты информации
	Умеет: Применяет методы защиты информации при выполнении задач профессиональной деятельности
	Владеет: Навыкамиприменения методов защиты информации при выполнении задач профессиональной деятельности

Результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные материалы
ОПК-3.2Применяет методы защиты информации при выполнении задач профессиональной деятельности	**Знает:** методы защиты информации	Задания (тесты 1-5)
	Умеет: Применяет методы защиты информации при выполнении задач профессиональной деятельности	Задания 1
	Владеет: Навыкамиприменения методов защиты информации при выполнении задач профессиональной деятельности	Задания 2

Промежуточная аттестация (зачет) проводится в одной из следующих форм:
1) собеседование;
2) выполнение заданий в ЭИОС СамГУПС.

2. Типовые[1] контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированности компетенций

2.1 Типовые вопросы (тестовые задания) для оценки знаниевого образовательного результата

Проверяемый образовательный результат

Код и наименование индикатора достижения компетенции	Образовательный результат
ОПК-3.2	Знает методы защиты информации

1.Чтоизнижеперечисленногоотноситсякпроблемаминформации(*выберитенесколькovариантовответа*)?

1) обеспечениецелостности;
2) обеспечениенеделимости;
3) обеспечениедостоверности;
4) обеспечениечистоты;
5) обеспечениезащитыотразличноговидаугроз.

2. Процесс обеспечения информационных потребностей общества на основе применения новейших информационных технологий — это…
1) компьютеризация;
2) информатика;
3) информатизация;
4) информационная индустрия;
5) автоматизация.

3. Информационная система — это…
1) посредник между потребителем информации и информационным массивом;
2) ряд компьютеров, объединенных в локальную сеть;
3) совокупность технических средств обработки информации;
4) группа людей, ответственная за обработку, накопление, хранение и выдачу информации;
5) средства массовой информации, функционирующие на территории определенного государства.

4. Какие свойства информации являются наиболее важными в практическом применении (выберите несколько вариантов ответа)?
1) ценность;
2) популярность;
3) достоверность;
4) чистота;
5) своевременность.

5. Что является основной причиной старения информации?
1) физическая изношенность носителя;
2) появление новой информации, с поступлением которой прежняя информация оказывается неверной;
3) устаревание знаковой системы, посредством которой выражена ин- формация;
4) уменьшение потребности в информации;
5) величина длительности хранения информации: чем больше длительность, тем информация старее.

6. Совокупность взаимосвязанных и взаимообусловленных процессов выявления, анализа, ввода и отбора информации, выдачи с помощью различных средств ее потребителю для принятия управленческого решения —

[1]Приводятся типовые вопросы и задания. Оценочные средства, предназначенные для проведения аттестационного мероприятия, хранятся на кафедре в достаточном для проведения оценочных процедур количестве вариантов. Оценочные средства подлежат актуализации с учетом развития науки, образования, культуры, экономики, техники, технологий и социальной сферы. Ответственность за нераспространение содержания оценочных средств среди обучающихся университета несут заведующий кафедрой и преподаватель – разработчик оценочных средств.

это…
1) процессы обработки информации;
2) циркуляция информации;
3) информационные процессы;
4) процессы перераспределения информации;
5) вычислительные процессы.

7. Организационно-упорядоченная совокупность людей, информационных ресурсов, технических средств и технологий обработки информации, имеющая своей целью сбор, обработку, накопление, хранение, актуализацию, поиск и выдачу информации — это…
1) автоматизированная инфраструктура;
2) информационная система;
3) информационная структура;
4) автоматизированная система;
6) информационный ресурс.

8.Что понимается под безошибочностью данных?
1) свойство данных не иметь явных ошибок;
2) свойство данных полностью соответствовать области их применения;
3) свойство данных не иметь скрытых случайных ошибок;
4) свойство данных соответствовать нескольким областям человеческой деятельности;
5) свойство данных не иметь противоречий в собственной структуре;

9. Назовите свойство данных, которое заключается в том, что время их сбора и переработки соответствует динамике изменения ситуации:
1) идентичность;
2) оперативность;
3) динамичность;
4) адаптивность;
5) актуальность.

10. Каким свойством обладают данные, соответствующие состоянию объекта (явления)?
1) идентичность;
2) объективность;
3) эквивалентность;
4) неотрывность;
5) целостность.

11. Что является источником информации, обладающей свойством «общественная природа»?
1) живые организмы, несущие в своем строении определенную биологическую информацию;
2) структура и состояние современного общества;
3) отношения между людьми;
4) познавательная деятельность людей, общества;
5) состояние окружающей среды.

12. Что подразумевается под целостностью информации (выберите не-сколько вариантов ответа)?
1) принадлежность информации одному источнику;
2) неделимость информации;
3) актуальность информации;
4) непротиворечивость информации;
5) защищенность информации от разрушения и несанкционированного изменения.

13. Меры каких уровней необходимо принимать при обеспечении за- щиты интересов субъектов информационных отношений?
1) социального;
2) законодательного;
3) исполнительного;

4) административного;
5) экономического;
6) процедурного;
7) функционального;
8) программно-технического;
9) программно-аппаратного.

14. Что относится к основным составляющим информационной безопасности (выберите несколько вариантов ответа)?
1) защита информации;
2) компьютерная безопасность;
3) экологическая безопасность;
4) защищенность информации и поддерживающей инфраструктуры;
5) защита от информации;
6) защищенность потребностей граждан.

15. Что относится к первоочередным задачам защиты информации (выберите несколько вариантов ответа)?
1) обеспечение качества информационных ресурсов;
2) обеспечение целостности информационных ресурсов;
3) обеспечение доступности информационных ресурсов;
4) обеспечение надежности информационных ресурсов;
5) обеспечение конфиденциальности информационных ресурсов.

16. Обозначьте основные направления деятельности на законодатель- ном уроне в сфере обеспечения информационной безопасности (выберите несколько вариантов ответа)?
1) разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
2) ориентация на созидательные законы;
3) ориентация на карательные законы;
4) создание уникальных стандартов и сертификационных нормативов, актуальных только в России;
5) интеграция в мировое правовое пространство;
6) учет современного состояния информационных технологий;
7) использование исключительно собственного опыта при создании нормативно-правовой базы в области информационной безопасности.

17. Выделите основные группы процедурных мер, направленных на обеспечение информационной безопасности (выберите несколько вариантов ответа).
1) программная защита;
2) управление персоналом;
3) управление ресурсами;
4) аппаратная защита;
5) физическая защита;
6) поддержание работоспособности;
7) реагирование на нарушения режима безопасности;
8) обеспечение стабильности;
9) планирование восстановительных работ.

18. На чем основывается политика информационной безопасности в организации?
1) на выявлении всех возможных угроз информационной безопасности организации;
2) на поиске уязвимостей информационной системы организации;
3) на анализе рисков, признанных реальными для информационной системы организации;
4) на закупке оборудования, предотвращающего утечку информации по техническим каналам;
5) на регистрации всех действий персонала при работе с защищаемой информацией.

19. Уполномоченными лицами считаются … (выберите несколько вариантов ответа)
1) собственники информации;
2) владельцы информации;
3) пользователи информации;

4) пользователи, получившие право работы с информацией от ее владельца;
5) государственные служащие;
6) работники силовых структур.

20. Уязвимость — это …
1) наличие узких мест в системе защиты информации;
2) слабость системы информационной безопасности;
3) незащищенность или ошибка в объекте, которая может привести к возникновению угрозы;
4) наличие угроз информационной безопасности;
5) незащищенность объектов информационной системы.

21. Неумышленное происшествие с деструктивным воздействием на объект — это …
1) ошибка;
2) катастрофа;
3) авария;
4) повреждение;
5) поломка.

22. Для чего предназначены информационные способы работы с ин- формационными потоками (выберите несколько вариантов ответа)?
1) сбор информации;
2) качественное, своевременное и достоверное удовлетворение информационных потребностей пользователей;
3) перераспределение информации;
4) передача информации;
5) уничтожение информации.

23. Основные компоненты информатизации включают в себя (выбери- те несколько вариантов ответа) …
1) оборудование;
2) вычислительные сети;
3) информационные системы;
4) каналы связи;
5) информационные ресурсы.

24. Информационные ресурсы — это…
1) документ, входящий в информационную систему;
2) массивы документов;
3) файлы, хранящиеся в памяти компьютера;
4) документы и массивы документов в разных формах и видах, содержащие информацию по всем направлениям жизнедеятельности общества;
5) все существующие знания.

25. Что из нижеперечисленного относится к свойствам информации (выберите несколько вариантов ответа)?
1) неотрывность от языка носителя;
2) дискретность;
3) периодичность;
4) независимость от создателей;
5) латентность.

26. Фиксированные информационные ресурсы — это…
1) некоторые сведения, которые не могут менять свое содержание со временем;
2) информация, закрепленная на каком-нибудь физическом носителе;
3) набор символов, имеющий смысл и определенную размерность;
4) фиксированный массив документов, необходимый для удовлетворения информационных потребностей общества в определенной сфере деятельности;
5) документы определенного вида.

27. Информация — это…
1) входные данные;

2) фиксированный набор символов естественного языка;
3) сведения о лицах, предметах, событиях, явлениях и процессах, хранящиеся в памяти ЭВМ;
4) сведения о лицах, предметах, событиях, явлениях и процессах, отраженные на материальных носителях, используемые в целях получения знаний и практических решений;
5) признаковая структура объектов.

28. Чем определяется ценность информации?
1) рыночной стоимостью;
2) обеспечением возможности достижения цели, поставленной перед получателем;
3) стоимостью носителя;
4) степенью доверия к источнику;
5) количеством заинтересованных в ней лиц.

29. Что такое защита информации?
1) создание защищенных банков данных конфиденциальной информации;
2) комплекс мероприятий по обеспечению конфиденциальности, целостности, доступности, учета и неотрекаемости информации;
3) набор аппаратных и программных средств для обеспечения конфиденциальности, целостности, доступности, учета и неотрекаемости информации;

4) комплекс мероприятий по обеспечению сохранности, доступности и конфиденциальности данных в компьютерных сетях;
5) обеспечение кодирования информации, передаваемой в локальной сети организации.

30. Возможность за приемлемое время получить требуемую информационную услугу определяет …
1) отказоустойчивость информационной системы;
2) время отклика системы;
3) пропускную способность канала;
4) качество сервиса;
5) степень доступности информации.

31. Что подразумевается под комплексом организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе?
1) информационная защищенность;
2) информационная стабильность;
3) стойкость информационной системы;
4) национальная безопасность;
5) информационная безопасность.
32. Что такое «угроза»?
1) возможность реализации несанкционированных действий в отношении информационной системы;
2) невосполнимый ущерб, нанесенный государственной организации;
3) предотвращенное деструктивное воздействие на информационную систему;
4) непоправимый вред, наносимый окружающей среде;
5) уязвимость информационной системы.

33. Назовите основные средства защиты информации (выберите не-сколько вариантов ответа):
1) электромеханические;
2) физические;
3) аппаратные;
4) виброакустические;
5) программные;
6) криптографические;
7) идентификационные.

34. Назовите свойство данных сохранять ценность для потребителя с течением времени, т.е. не подвергаться моральному старению:
1) актуальность;
2) значимость;

3) неизменность;
4) срочность;
5) постоянность.

35. Что понимается под совокупностью документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов?
1) информационная политика;
2) безопасность информации;
3) политика безопасности;
4) регламентация доступа;
5) организация защиты.

36. Какие механизмы безопасности необходимо использовать в рамках современных информационных систем (выберите несколько вариантов ответа)?
1) квотирование;
2) идентификация и аутентификация пользователей;
3) управление доступом;
4) резервное копирование;
5) протоколирование и аудит;
6) обеспечение высокой производительности системы;
7) обновление;
8) криптография;
9) межсетевое экранирование;
10) обеспечение высокой доступности.

37. Перечислите основные группы мер, которые необходимо реализовывать на законодательном уровне для обеспечения информационной без- опасности (выберите несколько вариантов ответа);
1) меры, направленные на увеличение количества аппаратно- программных продуктов иностранного производства на отечественном рынке;
2) меры, направленные на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности;
3) меры, направленные на снижение использования средств вычисли- тельной техники (СВТ) во всех сферах человеческой деятельности;
4) меры, направленные на ограничение доступа рядовых граждан к механизмам информационной безопасности;
5) меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

38. Фиксация и анализ всех действий уполномоченных лиц, выполняемых ими в рамках, контролируемых системой информационной безопасности
— это …
1) контроль;
2) учет;
3) база знаний;
4) слежка;
5) регистрация.

39. Попытка практической реализации угрозы — это …
1) взлом;
2) атака;
3) кража;
4) нападение;
5) удаленная атака.

40. Каким свойством обладают данные, характеризующие текущую ситуацию?
1) адаптивность;
2) корректность;

3) непротиворечивость;
4) целостность;
5) актуальность.

41. Субъект, преследующий корыстные или деструктивные цели, противоречащие целям системы, — это …
1) вредитель;
2) хакер;
3) агент конкурирующей системы;
4) правонарушитель;
5) злоумышленник.

42. Что понимается под истинностью данных?
1) свойство данных не иметь скрытых случайных ошибок;
2) свойство данных постоянно соответствовать текущей ситуации;
3) свойство данных противостоять деструктивному воздействию;
4) свойство данных не иметь явных ошибок;
5) свойство данных не иметь преднамеренные искажения человеком — источником сведений или искажения, вносимые средствами обработки информации.

43. Что представляет собой «информационная безопасность» в соответствии с Доктриной информационной безопасности Российской Федерации?
1) состояние системы, при котором она способна противостоять де- стабилизирующему воздействию внешних и внутренних информационных угроз;
2) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет,
территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;
3) состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства;
4) состояние информационной системы предприятия, при котором невозможно деструктивное воздействие на элементы данной системы со стороны сотрудников организации;
5) состояние защищенности информационных ресурсов от дестабилизирующего воздействия внешних и внутренних злоумышленников.

44. Что представляет собой объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы?
7) государственная информационная политика;
8) информационная безопасность Российской Федерации;
9) национальные интересы Российской Федерации в информационной сфере;
10) информационные интересы Российской Федерации;
11) национальная безопасность Российской Федерации в информационной сфере.

45. Что представляет собой совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства?
1) мировую экологическую обстановку;
2) злоумышленные действия вражеской разведки;
3) потенциальный вред;
4) угрозу;
5) промышленный шпионаж с привлечением разведывательных и специальных служб.

46. Что можно отнести к важнейшим принципам деятельности государственных органов по обеспечению информационной безопасности (выберите несколько вариантов ответа)?
1) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений;
2) предоставление гражданам информации по работе государственных органов на всех уровнях;
3) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной без- опасности;

4) соблюдение баланса между потребностью граждан в свободном об- мене информацией и ограничениями;
5) развитие систем массовой информации Российской Федерации.

47. Что можно отнести к внутренним угрозам информационной без- опасности в соответствии с Доктриной информационной безопасности Российской Федерации (выберите несколько вариантов ответа)?
1) расширение областей применения информационных технологий;
2) информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно- нравственных ценностей;
3) возрастающие масштабы компьютерной преступности;
4) целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем Российской Федерации;
5) высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи.

48. Что является стратегической целью обеспечения информационной безопасности в области обороны страны согласно Доктрине информационной безопасности Российской Федерации?
1) защита суверенитета;
2) поддержание обороноспособности Российской Федерации;
3) защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях;
4) поддержание территориальной целостности Российской Федерации;
5) обеспечение основных прав и свобод человека и гражданина.

49. Перечислите организации, которые входят в состав организационной основы системы обеспечения информационной безопасности Российской Федерации (выберите несколько вариантов ответа);
1) ФСБ России;
2) Совет Федерации Федерального Собрания РФ;
3) Совет Безопасности Российской Федерации;
4) ФСТЭК России;
5) Государственная Дума Федерального Собрания РФ;
6) МВД России;
7) Правительство РФ.

50. Основным органом, координирующим действия государственных структур по вопросам защиты государственной тайны, является;
1) Совет Безопасности Российской Федерации;
2) ФСБ России;
3) Межведомственная комиссия по защите государственной тайны;
4) СВР России;
5) Минобороны России;
6) Роскомнадзор.

51. Назовите организацию, координирующую деятельность государственной системы противодействия техническим разведкам и технической защиты информации:
1) ФСТЭК России;
2) ФСБ России;
3) ФСО России;
4) МВД России;
5) СВР России.

52. Что относится к основной деятельности Минобороны России в области обеспечения информационной безопасности?
1) разработка криптографических средств защиты информации;
2) организация деятельности по обеспечению информационной без- опасности, защите государственной тайны в Вооруженных Силах РФ;
3) организационно-техническое обеспечение деятельности Межведомственной комиссии по защите государственной тайны;

4) организация деятельности государственной системы противодействия техническим разведкам на федеральном уровне;
5) техническая защита информации в аппаратах федеральных органов государственной власти.

53. К угрозам информационной безопасности для личности можно отнести … (выберите несколько вариантов ответа)
1) препятствия в построении информационного общества;
2) манипулирование массовым сознанием;
3) лишение права граждан на неприкосновенность частной жизни;
4) противодействие защите интересов личности и общества;
5) нарушение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации.

54. К угрозам информационной безопасности для государства можно отнести … (выберите несколько вариантов ответа)
1) лишение права граждан на неприкосновенность частной жизни;
2) противодействие защите интересов личности и общества;
3) посягательства на объекты интеллектуальной собственности;

4) противодействие защите единого информационного пространства страны;
5) противодействие построению правового государства.

55. Что представляет собой «информационная сфера» в соответствии с Доктриной информационной безопасности Российской Федерации?
1) системообразующий фактор жизни общества, активно влияющий на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации;
2) совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной без- опасности, а также совокупность механизмов регулирования соответствующих общественных отношений;
3) федеральная государственная информационная система, порядок использования которой устанавливается Правительством РФ и которая обеспечивает в случаях, предусмотренных законодательством РФ, санкциониро-ванный доступ к информации, содержащейся в информационных системах;
4) совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений;
5) совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории РФ, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров РФ.

56. Национальными интересами Российской Федерации в информационной сфере являются (выберите несколько вариантов ответа):
1) защита государственных информационных ресурсов от несанкционированного доступа;
2) развитие в Российской Федерации отрасли информационных техно- логий и электронной промышленности;
3) обеспечение свободного сбора, хранения, использования и распространения информации о частной жизни граждан Российской Федерации;
4) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации;
5) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности.

57. Какие бывают уровни воздействия информационной безопасности (выберите несколько вариантов ответа)?
1) для личности;
2) для организации;
3) для государства;
4) для предприятия;
5) для общества;

6) для субъекта РФ.

58. Что можно отнести к важнейшим задачам государственных органов в рамках деятельности по обеспечению информационной безопасности (вы- берите несколько вариантов ответа)?
1) организация разведывательной деятельности для обеспечения ин- формационной безопасности личности, общества и государства;
2) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;
3) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;
4) государственная поддержка разработки, производства и эксплуатации средств информационного взаимодействия;
5) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности.

59. Что можно отнести к внешним угрозам информационной безопасности в соответствии с Доктриной информационной безопасности Российской Федерации (выберите несколько вариантов ответа)?
1) наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях;
2) отставание России от ведущих стран мира по уровню информатизации;
3) увеличение в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации;
4) отсутствие четко сформулированной информационной политики, отвечающей национальным целям, ценностям и интересам;
5) информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно- нравственных ценностей.

60. Что можно отнести к стратегическим целями обеспечения информационной безопасности в области государственной и общественной без- опасности согласно Доктрине информационной безопасности Российской Федерации (выберите несколько вариантов ответа)?

1) защита суверенитета;
2) поддержание обороноспособности Российской Федерации;
3) обеспечение секретности информационной структуры Российской Федерации;
4) поддержание территориальной целостности Российской Федерации;
5) обеспечение основных прав и свобод человека и гражданина.

61. Перечислите участников системы обеспечения информационной безопасности Российской Федерации согласно Доктрине информационной безопасности Российской Федерации (выберите несколько вариантов ответа);
1) федеральные и муниципальные органы власти;
2) собственники объектов критической информационной инфраструктуры;
3) средства массовой информации и массовых коммуникаций;
4) организации, осуществляющие образовательную деятельность;
5) организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка;
6) организации и граждане Российской Федерации;
7) операторы связи.

62. Какие государственные органы Российской Федерации контролируют деятельность в области информационной безопасности (выберите несколько вариантов ответа)?
1) СВР России;
2) Совет Безопасности Российской Федерации;
3) Государственная Дума Федерального Собрания РФ;
4) ФСТЭК России;
5) ФСБ России;
6) МВД России;
7) Правительство РФ.

63. Что относится к задачам ФСТЭК России в области обеспечения ин- формационной безопасности (выберите

несколько вариантов ответа)?
1) разработка отраслевых документов по защите информации;
2) противодействие добыванию информации техническими средства- ми разведки, техническая защита информации;
3) разработка криптографических методов защиты информации;
4) осуществление нормативно-правового регулирования вопросов технической защиты информации;
5) прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации.

64. Назовите организацию, обеспечивающую
безопасность информационно-телекоммуникационных систем криптографическими и инженерно-техническими методами;
1) ФСО России;
2) Минобороны России;
3) ФСБ России;
4) СВР России;
5) ФСТЭК России.

65. К угрозам информационной безопасности для общества можно от- нести … (выберите несколько вариантов ответа)
1) нарушение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации;
2) препятствия в построении информационного общества;
3) манипулирование массовым сознанием;
4) препятствие формированию институтов общественного контроля органов государственной власти;
5) противодействие защите государственных информационных систем и государственных информационных ресурсов.

66. По происхождению угрозы информационной безопасности бывают
… (выберите несколько вариантов ответа)
1) сторонние;
2) внезапные;
3) внутренние;
4) ожидаемые;
5) внешние.

67. Какая информация подлежит защите (выберите несколько вариантов ответа)?
1) информация, которая не подлежит разглашению;
2) секретная информация;
3) важная информация;
4) оперативная информация;
5) конфиденциальная информация.

68. Базовый федеральный закон, регулирующий информационные от- ношения — это Федеральный закон:
1) «Об информации, информационных технологиях и защите информации»;
2) «О коммерческой тайне»;
3) «Об архивном деле в Российской Федерации»;
4) «О связи».

69. Информация ограниченного доступа — это …
1) информация, доступ к которой ограничен федеральными законами;
2) информация, доступ к которой ограничен законами субъекта РФ;
3) информация, доступ к которой ограничен в силу указа ПрезидентаРФ;
4) информация, доступ к которой ограничен Конституцией РФ.

70. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам, — это …
1) обладатель информации;
2) создатель информации;

3) источник информации;
4) распространитель информации.

71. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию треть- им лицам без согласия ее обладателя — это:
1) конфиденциальность информации;
2) недоступность информации;
3) засекреченность информации;
4) защита информации.

72. К информации ограниченного доступа не относятся;
1) санитарно-эпидемиологическая информация;
2) коммерческая тайна;
3) персональные данные;
4) сведения о мерах безопасности в отношении судьи и участников уголовного процесса.

73. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации, — это;
1) секретная информация;
2) государственная тайна;
3) конфиденциальная информация;
4) совершенно секретная информация;
5) межгосударственная тайна.

74. Какой гриф секретности в соответствии с постановлением Правительства РФ от 4 сентября 1995 г. № 870 присваивается информации, распространение которой может нанести ущерб интересам министерства (федеральной службы) или отрасли экономики Российской Федерации?
1) секретная информация;
2) строго конфиденциальная информация;
3) совершенно секретная информация;
4) конфиденциальная информация;
5) информация особой важности.

75. Что относится к источникам информации?
1) отдельные материальные объекты;
2) субъекты, обладающие генетической памятью;
3) субъекты и объекты, обладающие определенной информацией, которая представляет конкретный интерес для злоумышленников или конкурентов;
4) определенные субъекты;
5) материальные носители информации, представляющей интерес только для специалистов определенных сфер деятельности.

76. Какую информацию относят к конфиденциальной (выберите несколько вариантов ответа)?
1) коммерческую тайну;
2) персональные данные;
3) государственную тайну;
4) тайну переписки;
5) ведомственную тайну;
6) тайну переговоров.

77. Как различается информация, относящаяся к разным степеням секретности?
1) временем получения данной информации;
2) степенью тяжести ущерба, наносимого утечкой данной информации;
3) объемом сведений;
4) количеством средств, затрачиваемых на ее получение потенциальным злоумышленником;
5) вычислительной мощностью, требующейся для ее декодирования.

78. Кто имеет право засекречивать информацию (выберите несколько вариантов ответа)?
1) органы власти;
2) должностные лица;
3) органы управления;
4) любой гражданин Российской Федерации;
5) Правительство РФ.

79. Сведения, не подлежащие засекречиванию (выберите несколько вариантов ответа):
1) о чрезвычайных происшествиях и катастрофах, угрожающих без- опасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
2) о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию войск, об их боеспособности и мобилизационной готовности, о создании и использовании мобилизационных ресурсов;
3) о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
4) научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность Российской Федерации;
5) о методах и средствах защиты секретной информации;
6) о состоянии здоровья высших должностных лиц Российской Федерации;
7) о фактах нарушения законности органами государственной власти и их должностными лицами.

80. На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные… (выберите несколько вариантов ответа)
1) о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;
2) гриф секретности информации;
3) об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;
4) о регистрационном номере;
5) об инвентарном номере;
6) список должностных лиц, допущенных к ознакомлению с содержащимися в этом носителе сведениями;
7) о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

81. Основанием рассекречивания сведений, составляющих государственную тайну, не является:
1) изменение срока засекречивания;
2) взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими государственную тайну;
3) истечение установленного срока засекречивания;
4) изменение объективных обстоятельств.

82. Целью защиты информации не является:
1) обеспечение использования информации;
2) предотвращение хищения, утечки, искажения, утраты и подделки информации;
3) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;
4) реализация права на государственную тайну и конфиденциальную информацию.

83. Степенью секретности информации не является:
1) ограниченность в доступе;
2) особая важность;
3) совершенно секретно;
4) секретно.

84. Каким требованиям отвечает информация, отнесенная к коммерческой тайне (выберите несколько вариантов ответа)?
1) имеет действительную или потенциальную ценность в силу ее неизвестности третьим лицам;

2) ее утечка может нанести ущерб безопасности Российской Федерации;
3) не подпадает под перечень сведений, доступ к которым не может
быть ограничен, и перечень сведений, отнесенных к государственной тайне;
4) ее цена не должна превышать 16 минимальных размеров оплаты труда (МРОТ);
5) к ней нет свободного доступа на законном основании;
6) ее ценность со временем не меняется;
7) обладатель принимает меры по охране ее конфиденциальности.

85. Что относится к основным объектам банковской тайны (выберите несколько вариантов ответа):
1) Государственная Дума Федерального Собрания РФ;
2) Президент РФ;
3) Министр внутренних дел РФ;
4) Правительство РФ;
5) органы судебной власти.

95. Должностные лица, принявшие решения о засекречивании сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от … (выберите несколько вариантов ответа)
1) причиненного обществу, государству и гражданам материального и морального ущерба;
2) причиненного ущерба, нанесенного экономике государства;
3) причиненного ущерба, нанесенного международному имиджу Российской Федерации;
4) причиненного ущерба инфраструктуре по обеспечению обороноспособности и безопасности Российской Федерации;
5) причиненного личности, обществу и государству материального ущерба.

96. Какая информация не может быть отнесена к коммерческой тайне (выберите несколько вариантов ответа)?
1) содержащая технологию производства;
2) содержащаяся в учредительных документах;
3) содержащая персональные данные граждан Российской Федерации;
4) содержащая сведения о задолженностях работодателей по выплате заработной платы и другим выплатам социального характера;
5) содержащая сведения о численности и кадровом составе работающих;
6) содержащая маркетинговую политику руководителя.

97. Что относится к основным объектам профессиональной тайны (вы- берите несколько вариантов ответа)?
1) тайна страхования;
2) тайна связи;
3) тайна контрагента;
4) тайна проповеди;
5) нотариальная тайна;
6) тайна покупателя.

98. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленном федеральными законами случаях, — это …
1) опознавательные признаки;
2) персональные данные;
3) открытые сведения;
4) биометрический паспорт;
5) база данных.

99. Что представляют собой угроза?
1) нестабильное состояние мировой экономики;
2) совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию информационных технологий или его собственнику;
3) совокупность условий и факторов, влияющих на циркуляцию ин- формации в каналах связи;
4) такое состояние информационной системы, при котором она, с од- ной стороны, не способна противостоять

дестабилизирующему воздействию внешних и внутренних факторов, а с другой — ее функционирование создает опасность для элементов самой системы и внешней среды.

100. Перечислите все возможные последствия реализации той или иной угрозы безопасности информации (выберите несколько вариантов ответа):
1) фиксация информации;
2) изменение информации;
3) уничтожение информации;
4) обновление информации;
5) хищение информации;
6) сокрытие информации;
7) блокирование информации.

101. Источниками угрозы информационной безопасности являются… (выберите несколько вариантов ответа)
1) потенциальные злоумышленники;
2) компрометирующие ситуации;
3) благоприятные факторы;
4) непредсказуемые последствия;
5) сложные обстоятельства.

102. К активным угрозам относятся:
1) попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания;
2) копирование информации;
3) разрушение или радиоэлектронное подавление линий связи, вывод из строя компьютера или операционной системы;
4) анализ графика.

103. Какие угрозы безопасности информации являются преднамеренными?
1) некомпетентное использование средств защиты;
2) поджог;
3) неумышленное повреждение каналов связи;
4) ошибки в программном обеспечении.

104. Что не относится к угрозам информационной безопасности?
1) классификация уязвимостей;
2) сбои и отказы оборудования (технических средств);
3) преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов);
4) хищение производственных отходов.

105. К посторонним лицам нарушителей информационной безопасности относятся:
1) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2) персонал, обслуживающий технические средства;
3) технический персонал, обслуживающий здание;
4) пользователи;
5) сотрудники службы безопасности;
6) представители конкурирующих организаций;
7) лица, нарушившие пропускной режим.

106. Искусственные угрозы безопасности информации вызваны:
1) деятельностью человека;
2) ошибками при проектировании компьютерных систем, ее элементов или разработке программного обеспечения;
3) воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4) корыстными устремлениями злоумышленников;
5) ошибками при действиях персонала.

107. К внутренним нарушителям информационной безопасности относится (выберите несколько вариантов ответа):
1) клиенты;
2) пользователи системы;
3) посетители;
4) любые лица, находящиеся внутри контролируемой территории;
5) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
6) персонал, обслуживающий технические средства;
7) сотрудники отделов разработки и сопровождения программного обеспечения;
8) технический персонал, обслуживающий здание.

108. Что можно отнести к угрозам случайных воздействий на источник информации (выберите несколько вариантов ответа)?
1) проявление стихии;
2) атаки хакеров;
3) действия помех;
4) сбои аппаратуры;
5) ошибки программ;
6) деструктивное воздействие со стороны обиженных сотрудников.

109. Какие действия пользователя информации и злоумышленника создают угрозу утечки информации (выберите несколько вариантов ответа)?
1) утеря источника информации (документа, продукции и др.);
2) разглашение сведений;
3) регулярная проверка помещений на наличие закладных устройств;
4) соблюдение режима коммерческой тайны в организации;
5) перехват электромагнитных полей и электрических сигналов, со- держащих защищаемую информацию;
6) утилизация всех отходов дело- и промышленного производства.

110. В каком случае возникает реальный ущерб?
1) при появлении угрозы;
2) при уничтожении уязвимости;
3) при реализации угрозы;
4) при организации защиты конфиденциальной информации;
5) при оценке вреда, наносимого той или иной угрозой.

111. Как называется попытка реализации угрозы безопасности информации?
1) нападение;
2) нарушение статичности;
3) атака;
4) обвал.

112. Какие угрозы безопасности информации являются преднамеренными?
1) ошибки персонала;
2) не авторизованный доступ;
3) открытие электронного письма, содержащего вирус;
4) любопытство.

113. К пассивным угрозам не относятся;
1) попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания;
2) копирование информации;
3) разрушение или радиоэлектронное подавление линий связи, вывод из строя компьютера или операционной системы;
4) анализ графика сети.

114. Какие угрозы безопасности информации являются непреднамеренными?
1) внедрение агентов в число персонала системы;
2) поджог;

3) умышленное повреждение каналов связи;
4) ошибки в программном обеспечении.

115. Что не относится к угрозам информационной безопасности?
1) классификация угроз;
2) вскрытие шифров криптозащиты информации;
3) нелегальное внедрение и использование неучтенных программ с по следующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
4) ввод ошибочных данных.

116. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
1) сотрудники;
2) хакеры;
3) атакующие;
4) контрагенты (лица, работающие по договору);
5) хактевисты;
6) кибершпионы.

117. Естественные угрозы безопасности информации вызваны…
1) деятельностью человека;
2) ошибками при проектировании компьютерной системы, ее элементов или разработке программного обеспечения;
3) воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4) корыстными устремлениями злоумышленников;
5) ошибками при действиях персонала.

118. Воздействия, которые создаются злоумышленниками, являются…
1) точечными;
2) разрушительными;
3) преднамеренными;
4) спровоцированными;
5) губительными.

119. Угрозы, приводящие к несанкционированному распространению носителя с защищаемой информацией к злоумышленнику, называются…
1) угрозами модификации информации;
2) угрозами утечки информации;
3) угрозами разрушения информации;
4) угрозами проявления стихии;
5) угрозами действия помех.

120. В каком случае возникает потенциальный ущерб?
1) при реализации угрозы;
2) при появлении угрозы;
3) при уничтожении уязвимости;
4) при организации защиты конфиденциальной информации;
5) при оценке вреда, наносимого той или иной угрозой.

121. В каком случае реализуется угроза утечки информации?
1) происходит утеря источника информации;
2) происходит частичная модификация защищаемой информации;
3) защищаемая информация полностью уничтожена;
4) информация попадает к злоумышленнику;
5) защищаемая информация теряет актуальность.

122. Из нижеперечисленного выделите возможные способы получения информации (выберите несколько

вариантов ответа):
1) изучение порядка сдачи налоговой отчетности предприятия;
2) изучение продукции предприятия;
3) ознакомление с правилами пожарной безопасности предприятия;
4) использование сведений, распространяемых служащими предприятия;
5) непосредственное наблюдение, осуществляемое скрытно.

123. Перечислите способы несанкционированного доступа к конфиденциальной информации (выберите несколько вариантов ответа):
1) авторизованный вход в систему;
2) хищение;
3) перехват;
4) актуализация базы данных;
5) копирование.

124. Перехват, который осуществляется путем использования оптической техники, называется…
1) активный перехват;
2) пассивный перехват;
3) аудиоперехват;
4) видеоперехват;
5) просмотр мусора.

125. Что понимается под «разглашением» конфиденциальной информации?
1) умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним;
2) передача сведений конфиденциального характера их обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены данным договором;
3) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена;
4) ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя при условии сохранения конфиденциальности данной информации.

126. Что относится к формальным каналам распространения информации (выберите несколько вариантов ответа)?
1) деловые встречи;
2) совещания;
3) личная переписка;
4) интернет;
5) телевидение.

127. «Утечка» конфиденциальной информации — это…
1) противоправное преднамеренное овладение конфиденциальной информацией;
2) умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним;
3) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена;
4) ознакомление определенных лиц с конфиденциальной информацией с согласия ее обладателя.

128. Что образуют внешние воздействия (силы), которые могут изменить, уничтожить информацию или привести к ее хищению, при распространении от источника внешнего воздействия до источника информации?
1) технический канал утечки информации;
2) канал несанкционированного доступа;
3) среду распространения носителя информации;
4) канал преобразования информации;
5) опасный сигнал.

129. Перечислите основные виды каналов утечки информации (выберите несколько вариантов ответа):
1) визуально-оптические;

2) магнитоконтактные;
3) акустические;
4) электромеханические;
5) электромагнитные;
6) материально-вещественные;
7) оптико-электронные.

130. Что подразумевается под «несанкционированным доступом» к конфиденциальной информации?
1) умышленные или
неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним;
2) противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам;
3) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена;
4) ознакомление определенных лиц с конфиденциальной информацией с согласия ее обладателя.

131. Как называется процесс приема и анализа акустических сигналов?
1) наблюдение;
2) перехват;
3) хищение;
4) фиксация;
5) подслушивание.

132. Как называется процесс приема и анализа радио- и электрических сигналов?
1) демодуляция;
2) консервация;
3) перехват;
4) преобразование;
5) регистрация.

133. Как называются сигналы, содержащие секретную или конфиденциальную информацию, которые могут быть перехвачены злоумышленником и с которых может быть снята данная информация?
1) модулированные сигналы;
2) дискретные сигналы;
3) полезные сигналы;
4) опасные сигналы;
5) секретные сигналы.

134. Активный перехват информации — это перехват, который…
1) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3) неправомерно использует технологические отходы информационного процесса;
4) осуществляется путем использования оптической техники;
5) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

135. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций, называется…
1) активный перехват;
2) пассивный перехват;
3) аудиоперехват;
4) видеоперехват;
5) просмотр мусора.

136. Степень опасности источника информации определяется …
1) размером потенциальных затрат злоумышленника на проникновение к данному источнику информации;
2) количеством способов несанкционированного доступа к источнику информации;

3) величиной доступности данного источника, определяемой эксперт- ной комиссией;
4) количеством информации, содержащимся в этом источнике;
5) размером ущерба, наносимого при использовании данного источника.

137. Что относится к неформальным каналам распространения информации (выберите несколько вариантов ответа)?
1) обмен официальными деловыми документами;
2) конференции;
3) выставки;
4) газеты;
5) средства передачи официальной информации.

138. Посредством чего осуществляется утечка конфиденциальной информации?
1) посредством активных соединений;
2) посредством организационных мероприятий;
3) посредством формальных коммуникаций;
4) посредством различных технических каналов;
5) посредством неформальных коммуникаций.

139. Что подразумевается под каналом утечки информации?
1) физический путь от источника информации к ее получателю;
2) физический путь от источника конфиденциальной информации к злоумышленнику;
3) материальные объекты, в том числе физические поля, в которых конфиденциальная информация находит свое отображение;
4) часть пространства, в которой перемещается носитель информации.

140. Перечислите основные способы несанкционированного доступа (выберите несколько вариантов ответа);
1) уничтожение носителей информации;
2) подслушивание телефонных переговоров;
3) порча средств вычислительной техники;
4) кража документов;
5) проникновение в компьютер.

141. Что из нижеперечисленного относится к условиям, способствующим неправомерному овладению конфиденциальной информацией (выбери- те несколько вариантов ответа)?
1) создание в организации должностной инструкции о порядке работы с конфиденциальной информацией;
2) излишняя болтливость сотрудников;
3) жесткий контроль обеспечения информационной безопасности в организации;
4) традиционный обмен производственным опытом;
5) бесконтрольное использование информационных систем;
6) случайный подбор кадров;
7) введение в организации режима коммерческой тайны.
142. Как называется прием оптических и иных сигналов от объектов и получение с их помощью изображений этих объектов?
1) подслушивание;
2) наблюдение;
3) перехват;
4) фиксация;
5) регистрации.

143. Как называется технический канал утечки информации, организованный злоумышленником установкой на объекте закладного устройства?
1) случайным;
2) потенциальным;
3) спонтанным;
4) опасным;
5) организованным.

144. Какие технические средства из нижеперечисленных создают опасные сигналы (выберите несколько вариантов ответа)?
1) электрические розетки;
2) средства телефонной проводной связи;
3) лампы накаливания;
4) средства электронной вычислительной техники;
5) видеоаппаратура.

145. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации, называется…
1) активный перехват;
2) пассивный перехват;
3) аудиоперехват;
4) видеоперехват;
5) просмотр мусора.

146. Способ несанкционированного доступа к источникам конфиденциальной информации называется — это:
1) потенциальные или реальные действия, приводящие к моральному или материальному ущербу;
2) спонтанное не зависящее от воли людей обстоятельство, возникающее в процессе ее функционирования, приводящее к утечке информации;
3) совокупность приемов и порядок действий с целью получения (добывания) охраняемых сведений незаконным, противоправным путем;
4) негативное воздействие на систему в целом или отдельные ее эле- менты, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде.

147. Какая информация добывается посредством подслушивания (выберите несколько вариантов ответа)?
1) информация об излучениях, модулированных звуковой волной;
2) информация о координатах источника звука;
3) речевая информация;
4) демаскирующие признаки сигналов различных источников звуков;
5) информация о направлении звуковой волны.

148. Назовите основной недостаток визуально-оптического наблюдения в видимом и инфракрасных диапазонах;
1) невозможность сохранения изображения для последующего анализа специалистами;
2) невозможность распознавания объекта в темное время суток;
3) невозможность наблюдения скрытых объектов через отверстия или щели;
4) недопустимо малое возможное расстояние до объекта.

149. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации — …
1) защищаемая информация;
2) конфиденциальная информация;
3) секретная информация;
4) информация ограниченного доступа.

150. Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров — …
1) объект информатизации;
2) информационная система;
3) комплексная защита объектов информатизации;
4) аттестованная информационная система.

3. Методические материалы, определяющие процедуру и критерии оценивания сформированности компетенций при проведении промежуточной аттестации

Критерии формирования оценок по ответам на вопросы, выполнению тестовых заданий

- оценка **«отлично»** выставляется обучающемуся, если количество правильных ответов на вопросы составляет 100 – 90% от общего объёма заданных вопросов;

- оценка **«хорошо»** выставляется обучающемуся, если количество правильных ответов на вопросы – 89 – 76% от общего объёма заданных вопросов;

- оценка **«удовлетворительно»** выставляется обучающемуся, если количество правильных ответов на тестовые вопросы –75–60 % от общего объёма заданных вопросов;

- оценка **«неудовлетворительно»** выставляется обучающемуся, если количество правильных ответов – менее 60% от общего объёма заданных вопросов.

Критерии формирования оценок по результатам выполнения заданий

«Отлично/зачтено» – ставится за работу, выполненную полностью без ошибок и недочетов.

«Хорошо/зачтено» – ставится за работу, выполненную полностью, но при наличии в ней не более одной негрубой ошибки и одного недочета, не более трех недочетов.

«Удовлетворительно/зачтено» – ставится за работу, если обучающийся правильно выполнил не менее 2/3 всей работы или допустил не более одной грубой ошибки и двух недочетов, не более одной грубой и одной негрубой ошибки, не более трех негрубых ошибок, одной негрубой ошибки и двух недочетов.

«Неудовлетворительно/не зачтено» – ставится за работу, если число ошибок и недочетов превысило норму для оценки «удовлетворительно» или правильно выполнено менее 2/3 всей работы.

Виды ошибок:

- грубые ошибки: незнание основных понятий, правил, норм; незнание приемов решения задач; ошибки, показывающие неправильное понимание условия предложенного задания.

- негрубые ошибки: неточности формулировок, определений; нерациональный выбор хода решения.

- недочеты: нерациональные приемы выполнения задания; отдельные погрешности в формулировке выводов; небрежное выполнение задания.

Критерии формирования оценок по зачету с оценкой

«Отлично/зачтено» – студент приобрел необходимые умения и навыки, продемонстрировал навык практического применения полученных знаний, не допустил логических и фактических ошибок

«Хорошо/зачтено» – студент приобрел необходимые умения и навыки, продемонстрировал навык практического применения полученных знаний; допустил незначительные ошибки и неточности.

«Удовлетворительно/зачтено» – студент допустил существенные ошибки.

«Неудовлетворительно/не зачтено» – студент демонстрирует фрагментарные знания изучаемого курса; отсутствуют необходимые умения и навыки, допущены грубые ошибки.

Экспертный лист
оценочных материалов для проведения промежуточной аттестации по
дисциплине «Основы информационной безопасности»

Направление подготовки / специальность

09.03.01 «Информатика и вычислительная техника»
(код и наименование)

Направленность (профиль)/специализация

_____
(наименование)

Бакалавр
квалификация выпускника

1. Формальное оценивание			
Показатели		Присутствуют	Отсутствуют
Наличие обязательных структурных элементов:		+	
–титульный лист		+	
–пояснительная записка		+	
– типовые оценочные материалы		+	
–методические материалы, определяющие процедуру и критерии оценивания		+	
Содержательное оценивание			
Показатели	Соответствует	Соответствует частично	Не соответствует
Соответствие требованиям ФГОС ВО к результатам освоения программы	+		
Соответствие требованиям ОПОП ВО к результатам освоения программы	+		
Ориентация на требования к трудовым функциям ПС (при наличии утвержденного ПС)	+		
Соответствует формируемым компетенциям, индикаторам достижения компетенций	+		

Заключение: ФОС рекомендуется/ не рекомендуется к внедрению; обеспечивает/ не обеспечивает объективность и достоверность результатов при проведении оценивания результатов обучения; критерии и показатели оценивания компетенций, шкалы оценивания обеспечивают/ не обеспечивают проведение всесторонней оценки результатов обучения.