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

Кафедра защиты информации

“УТВЕРЖДАЮ
” ДЕКАН АВТФ к.т.н.,
доцент И.Л. Рева
“ ___ ” _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

Защищенные информационные системы

Образовательная программа: 10.04.01 Информационная безопасность, профиль: Методы и средства обеспечения технической защиты информации

Новосибирск - 2023

1. Методика оценки этапов формирования компетенций по дисциплине

Результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций проверяются при проведении мероприятий текущей аттестации (контроля) в процессе изучения дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 3 семестре - в форме экзамена, который направлен на оценку сформированности результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенций ОПК-1 и соотнесенных с ними индикаторов.

Экзамен проводится в форме письменного тестирования с использованием электронной информационно-образовательной среды НГТУ (http:// www.nstu.ru/sveden/eos).

Общие правила выставления оценок текущей и промежуточной аттестации по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании критериев, приведенных в п. 2, осуществляется оценка уровней достигнутых результатов обучения по дисциплине, соотнесенных с установленными в программе индикаторами достижения компетенции ОПК-1, закрепленных за дисциплиной.

2. Общая характеристика уровней результатов обучения, соотнесенных с индикаторами достижения компетенций

Продвинутый. Теоретическое содержание курса освоено полностью. Студент демонстрирует систематическое и глубокое понимание учебного материала и способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. Сформированы необходимые навыки практической работы. Все учебные задания, предусмотренные программой обучения, выполнены качественно, без замечаний. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящим в диапазон продвинутого уровня.

Базовый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Навыки практической работы сформированы на базовом уровне. Все предусмотренные программой обучения учебные задания выполнены с небольшими погрешностями. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах базового уровня.

Пороговый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Некоторые практические навыки работы с сформированы с пробелами. Учебные задания, предусмотренные программой обучения, выполнялись с ошибками, исправленными под руководством преподавателя. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов в пределах порогового уровня.

Ниже порогового. Теоретическое содержание курса освоено фрагментарно. Необходимые навыки практической работы сформированы минимально. Большинство учебных заданий, предусмотренных программой обучения, не выполнены. Результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций, оценены числом баллов, входящих в диапазон ниже порогового уровня.

Паспорт экзамена

по дисциплине «Защищенные информационные системы», 3 семестр

1. Методика оценки Экзамен проводится в форме письменного тестирования с использованием электронной информационно-образовательной среды НГТУ (http:// www.nstu.ru/sveden/eos).

Тестовые задания охватывают все содержание дисциплины «Защищенные информационные системы».

Тест состоит из вопросов различного вида и позволяет проверить результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций.

2. Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций

Выполнение теста засчитывается на **продвинутом** уровне, если студент правильно ответил на 5/6 вопросов теста, знает определения всех понятий, продемонстрировал способность безошибочно устанавливать последовательность и соответствие между процессами и явлениями, выявлять проблемы, предлагать механизмы их решения, представляет количественные и качественные характеристики определенных процессов и не допускает ошибок при решении задач. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций не содержит пробелов. Установленные в программе компетенции сформированы в полном объеме. Оценка составляет *от 35 до 40 баллов.*

Выполнение теста засчитывается на **базовом** уровне, если студент правильно ответил на 2/3 вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, правильно характеризует процессы, явления, не допускает существенных ошибок при решении задач. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от 34 до 27 баллов.*

Выполнение теста засчитывается на **пороговом** уровне, если студент правильно ответил от 1/2 до 2/3 вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, при решении задач допускает непринципиальные ошибки, например, вычислительные. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от 26 до 20 баллов.*

Выполнение теста считается **неудовлетворительным**, если студент правильно ответил менее чем на половину вопросов теста, не знает определений понятий, не продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, при решении задач допускает принципиальные ошибки. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее 20 баллов.*

3. Шкала оценки Экзамен считается сданным, если сумма баллов по всем заданиям билета составляет от 20 до 40 баллов включительно. Сумма менее 20 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

4. Фонд оценочных материалов (вопросы теста[1]) для оценки уровня сформированности компетенций и соотнесенных с ними индикаторов

Формируемая компетенции	Индикаторы компетенции
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	2. владеет навыками участия в разработке системы обеспечения информационной безопасности объекта 3. умеет проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности от утечки по техническим каналам 4. умеет проектировать информационные системы с учетом различных технологий обеспечения информационной безопасности от несанкционированного доступа

Вопросы теста для оценки сформированности компетенции ОПК-1

Вопрос 1. В информационной системе объектами защиты являются

- **информация, содержащаяся в информационной системе ✓**
- документы, утвержденные руководством.
- письменные инструкции по эксплуатации системы.
- программное обеспечение и сетевые подключения.

(один вариант)

Вопрос 2. Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в какой форме? *Ответ:*

Решение: обязательной сертификации.

Вопрос 3. Для определения угроз безопасности информации и разработки модели угроз безопасности информации какие документы применяются? *Ответ:*

Решение: методические

Вопрос 4. Внедрение системы защиты информации информационной системы включает:

- **установку и настройку средств защиты информации в информационной системе ✓**
- замену устаревшего оборудования на более новое.
- разработку пользовательского интерфейса.
- покупку и установку антивирусного программного обеспечения.

(один вариант)

Вопрос 5. В качестве исходных данных, необходимых для аттестации информационной системы, используются

- **техническое задание на создание системы защиты информации информационной системы ✓**
- персональные данные пользователей системы.
- отчёты о финансовой деятельности организации.

○ стратегические планы развития организации.

(один вариант)

Вопрос 6. Организационные и технические меры защиты информации должны быть направлены на исключение:

- ☐ обновления программного обеспечения
- ☐ **неправомерных уничтожения или модифицирования информации ✓**
- ☐ резервного копирования данных
- ☐ формирование требований к защите информации

(один вариант)

Вопрос 7. Вставьте пропущенное слово.

Классификация информационной системы проводится по _____ обрабатываемой в системе информации.

Решение: значимости

Вопрос 8. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

- ○ **управления (администрирования) системой защиты информации информационной системы**
- ○ по использованию офисной техники и программного обеспечения.
- ○ по обеспечению комфортных условий труда сотрудников.
- ○ подбора и обучения персонала.

(один вариант)

Вопрос 9. В соответствии с чем проводится аттестация информационной системы?

- ○ **с программой и методиками аттестационных испытаний**
- ○ мнением пользователей системы
- ○ скоростью интернет-соединения
- ○ количеством пользователей системы

(один вариант)

Вопрос 10. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- ☐ использование одного и того же пароля администратора для всех систем
- ☐ **разработка системы защиты информации информационной системы**
- ☐ размещение серверов в общедоступных местах для удобства доступа
- ☐ неправомерное уничтожения или модифицирования информации

(один вариант)

Вопрос 11. При определении угроз безопасности информации учитываются:

- **структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы ✓**
- о предпочтения пользователей в использовании программного обеспечения.
- о планы развития организационной структуры компании.
- законодательные акты текущего года.

(один вариант)

Вопрос 12. При макетировании и тестировании системы защиты информации информационной системы осуществляются:

- **проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами ✓**
- оценка удобства интерфейса пользователя.
- проверка соответствия системы законодательным требованиям.
- написание кода для новых функций информационной системы.

(один вариант)

Вопрос 13. При внедрении организационных мер защиты информации осуществляются:

- **реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей ✓**
- разработка и внедрение технических средств защиты.
- проверка эффективности установленного антивирусного программного обеспечения.
- модернизация физической инфраструктуры объектов.

(один вариант)

Вопрос 14. При проведении аттестационных испытаний должны применяться следующие методы проверок (испытаний):

- анализ уязвимостей информационной системы, в том числе вызванных неправильной
- **настройкой (конфигурированием) программного обеспечения и средств защиты информации ✓**
- опрос пользователей для оценки удобства программного обеспечения.
- сравнение функциональности с конкурирующими системами.

(один вариант)

Вопрос 15. Устанавливаются три класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс?

- **третий класс защищенности**
- второй класс

- первый класс
- нет правильного ответа

(один вариант)

Вопрос 16. Что содержит модель угроз безопасности информации информационной системы? *Ответ:*

Решение: описание информационной системы.

Вопрос 17. Описание чего должна содержать эксплуатационная документация на систему защиты информации информационной системы?

- описание структуры системы защиты информации информационной системы
- информации, программного обеспечения и технических средств
- правила эксплуатации системы защиты информации информационной системы
- **все варианты верны✓**

(один вариант)

Вопрос 18. Допускается ли аттестация информационной системы на основе результатов аттестационных испытаний выделенного набора сегментов информационной системы? *Ответ:*

Решение: да.

Вопрос 19. Формирование требований к защите информации включает:

- принятие решения о необходимости защиты информации
- **все варианты верны ✓**
- безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации
- классификацию информационной системы по требованиям защиты информации
- определение требований к системе защиты информации информационной системы

(один вариант)

Вопрос 20. Что включает в себя описание угроз безопасности информации?

- **информация о потенциальных уязвимостях и способы реализации угроз безопасности информации. ✓**
- перечень используемого антивирусного программного обеспечения
- данные о частоте обновления программного обеспечения
- список сотрудников, ответственных за информационную безопасность

(один вариант)

Вопрос 21. При проектировании системы защиты информации информационной системы:

- **определяются типы субъектов доступа и объектов доступа, являющихся объектами защиты. ?**
- только выбор средств защиты информации
- разработка политик обеспечения физической безопасности
- интеграция мер по предотвращению внутренних угроз

(один вариант)

Вопрос 22. Дополните предложение: Анализ уязвимостей информационной системы проводится в целях ____ _____ реализации угроз *Ответ:*

Решение:. оценки предотвращения

Вопрос 23. Дополните предложение: Сегмент считается соответствующим сегменту информационной системы, в отношении которого были проведены аттестационные испытания, если установлены одинаковые ____ _____ *Ответ:*

Решение:. классы защищенности

Вопрос 24. Устанавливаются три класса защищенности информационной системы, определяющие уровни защищенности, содержащейся в ней информации. Самый высокий класс?

- третий класс
- второй класс
- **первый класс защищенности**
- нет правильного ответа

(один вариант)

Вопрос 25. Требования к системе защиты информации информационной системы должны содержать:

- **перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система ✓**
- перечень программного обеспечения компании
- руководство пользователя по работе с программным обеспечением
- план обучения пользователей работе с новыми программами

(один вариант)

Вопрос 26. Что нужно рассматривать при анализе уязвимостей информационной системы?

- Средства защиты информации
- Технические средства
- Программное обеспечение информационной системы
- **Все ответы верны**

(один вариант)

Вопрос 27. Угрозы безопасности информации определяются по результатам

- оценки возможностей (потенциала) внешних и внутренних нарушителей
- анализа возможных уязвимостей информационной системы
- возможных способов реализации угроз безопасности информации
- **Все ответы верны**

(один вариант)

Вопрос 28. Что учитывается при определении требования к системе защиты информации информационной системы?

Ответ:

Решение: класс защищенности

Вопрос 29. Кто является инициатором аттестация информационной системы? *Ответ:*

Решение: заказчик

Вопрос 30. Вставьте пропущенное слово. Аттестация информационной системы включает в себя _____ аттестационных испытаний.

Решение: Комплекс

Вопрос 31. Допускается ли проведение аттестационных испытаний информационной системы должностными лицами (работниками), осуществляющими проектирование и (или) внедрение системы защиты информации информационной системы? *Ответ:*

Решение: да

Вопрос 32. Обеспечение защиты информации в ходе эксплуатации информационной системы должно включать следующие мероприятия:

- планирование мероприятий по защите информации в информационной системе
- анализ угроз безопасности информации в информационной системе
- управление (администрирование) системой защиты информации информационной системы
- управление конфигурацией информационной системы и ее системой защиты информации
- **Все ответы верны ✓**

(один вариант)

Вопрос 33. В ходе управления (администрирования) системой защиты информации информационной системы осуществляются:

- определение лиц, ответственных за управление (администрирование) системой защиты информации информационной системы
- разграничения доступа в информационной системе
- управление средствами защиты информации информационной системы
- **Все ответы верны ✓**

(один вариант)

Вопрос 34. Вставьте пропущенное слово. Реализованные процессы _____ изменениями информационной системы и ее системы защиты информации должны включать процессы гарантийного и (или) технического обслуживания.

Решение: управления

Вопрос 35. В ходе реагирования на инциденты осуществляются:

- обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору

информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов

- своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
- **Все ответы верны ✓**

(один вариант)

Вопрос 36. Что нужно делать в ходе информирования и обучения персонала информационной системы?

- **информирование персонала информационной системы о появлении актуальных угрозах безопасности информации, о правилах безопасной эксплуатации информационной системы ✓**
- предоставление информации о последних изменениях в корпоративной культуре
- инструктаж по эксплуатации пожарных сигнализаций

(один вариант)

Вопрос 37. Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа
- контроль (анализ) защищенности информации
- целостность информационной системы и информации
- управление доступом субъектов доступа к объектам доступа
- **Все ответы верны ✓**

(один вариант)

Вопрос 38. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать

- **разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа ✓**
- непрерывность работы информационной системы
- нет правильного ответа

(один вариант)

Вопрос 39. Что должны исключать меры по защите машинных носителей информации? *Ответ:*

Решение: несанкционированный доступ.

Вопрос 40. Что обеспечивают меры по антивирусной защите?

- обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации.
- обнаружение программ для нейтрализации средств защиты информации
- реагирование на обнаружение программ и информации
- **Все ответы верны ✓**

(один вариант)

Вопрос 41. Меры по обнаружению (предотвращению) вторжений должны обеспечивать:

- увеличение времени отклика системы безопасности
- **обнаружение и реагирование на несанкционированные попытки доступа к информационным ресурсам✓**
- автоматическое удаление критически важной информации при обнаружении атаки
- создание искусственных узких мест в сети для снижения скорости передачи данных

(один вариант)

Вопрос 42. Меры по контролю (анализу) защищенности информации должны обеспечивать:

- ограничение доступа сотрудников к интернету
- постоянное наблюдение за пользователями системы
- **регулярное выявление и устранение уязвимостей и потенциальных угроз в системе безопасности ✓**
- отключение устройств хранения информации после рабочего времени

(один вариант)

Вопрос 43. Меры по обеспечению доступности информации должны обеспечивать:

- периодическое отключение системы для предотвращения перегрузок
- **гарантирование непрерывного доступа к информации для уполномоченных пользователей ✓**
- увеличение сложности процедур доступа для повышения безопасности
- размещение всех данных в одном месте для удобства доступа

(один вариант)

Вопрос 44. Меры по защите технических средств должны исключать:

- регулярное обновление антивирусных баз
- использование шифрования данных
- **несанкционированный доступ к оборудованию и данным ✔**

- применение сильных паролей и многофакторной аутентификации

(один вариант)

Вопрос 45. Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

- определение базового набора мер защиты информации для установленного класса защищенности информационной системы в соответствии с базовыми наборами мер защиты информации.
- адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы
- уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации
- **Все ответы верны ✓**

(один вариант)

Вопрос 46. В ходе планирования мероприятий по защите информации в информационной системе осуществляются:

- определение лиц, ответственных за планирование и контроль мероприятий по защите информации в информационной системе
- определение лиц, ответственных за выявление инцидентов и реагирование на них
- разработка, утверждение и актуализация плана мероприятий по защите информации в информационной системе
- **все ответы верны ✔**

(один вариант)

Вопрос 47. В ходе анализа угроз безопасности информации в информационной системе в ходе ее эксплуатации осуществляются:

- ☐ выявление, анализ и устранение уязвимостей информационной системы
- ☐ анализ изменения угроз безопасности информации в информационной системе
- ☐ оценка возможных последствий реализации угроз безопасности информации в информационной системе
- ☐ **все варианты верны ?**

(один вариант)

48. В ходе управления конфигурацией информационной систем и ее системы защиты информации осуществляются:

- ☐ определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и ее системы защиты информации, и их полномочий
- ☐ определение компонентов информационной системы и ее системы защиты информации, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю

- ☐ управление изменениями информационной системы и ее системы защиты информации: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в информационную систему и ее систему защиты информации, документирование действий по внесению изменений в информационную систему и сохранение данных об изменениях конфигурации
- ☐ **все варианты верны**

(один вариант)

Вопрос 49. В ходе контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

- ☐ контроль (анализ) защищенности информации с учетом особенностей функционирования информационной системы.
- ☐ анализ и оценка функционирования информационной системы и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты информации информационной системы
- ☐ документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе
- ☐ **все варианты верны**

(один вариант)

Вопрос 50. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации включает:

- o передачу всех данных конкурентам для анализа конкурентной среды
- o **архивирование информации, удаление всех данных без возможности восстановления** ✔
- o продолжение их использования без каких-либо изменений в режиме защиты
- o перемещение всех устройств хранения в незащищенное помещение

(один вариант)

Вопрос 51. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать

- ☐ присвоение субъектам и объектам доступа уникального признака (идентификатора)
- ☐ сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов
- ☐ проверка принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности)
- ☐ **все ответы верны** ✓

(один вариант)

Вопрос 52. Что должны обеспечивать меры по ограничению программной среды?

- ☐ исключать установку и запуск только разрешенного к использованию в информационной системе программного обеспечения
- ☐ **исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения** ✓
- ☐ нет правильного ответа

(один вариант)

Вопрос 53. Меры по регистрации событий безопасности должны обеспечивать:

- полное исключение риска возникновения инцидентов безопасности
- активное предотвращение атак на информационную систему
- **точность, полноту и своевременность записи информации о событиях безопасности✓**
- автоматическую ликвидацию последствий любых инцидентов безопасности

Вопрос 54. Что входит в меры по обеспечению целостности информационной системы и информации?

- ☐ **обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации ✓**
- ☐ мониторинг социальных сетей сотрудников
- ☐ увеличение объема хранения данных
- ☐ установка программ для учета рабочего времени сотрудников

(один вариант)

Вопрос 55. Что должны исключать меры по защите среды виртуализации?

Ответ:

Решение: несанкционированный доступ к информации.

Вопрос 56. Вставьте пропущенное слово. Защиту информации должны обеспечивать ____ по защите информационной системы, ее средств, систем связи и передачи данных при взаимодействии с другой информационной системой.

Решение: меры

Вопрос 57. В информационных системах какого класса защищённости обязана обеспечиваться защита от угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже усиленного базового?

- В информационных системах 3 класса
- В информационных системах 1 класса
- **В информационных системах 2 класса защищенности ✓**

(один вариант)

Вопрос 58. Средства защиты информации и средства вычислительной техники какого класса применяются в информационных системах 1 класса защищенности?

- ☐ **В информационных системах 1 класса защищенности применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса ✓**
- ☐ В информационных системах 1 класса защищенности применяются средства защиты информации 2 класса
- ☐ В информационных системах 1 класса защищенности применяются средства защиты информации 6 класса

(один вариант)

Вопрос 59. В информационных системах 1 класса защищенности какой уровень средств защиты информации применяется? *Ответ:*

Решение: 4 и выше.

Вопрос 60. В информационных системах 2 класса защищенности какой уровень средств защиты информации применяются? *Ответ:*

Решение: 5 и выше.