МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Луганский государственный университет имени Владимира Даля»

КОЛЛЕДЖ

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации
в форме дифференцированного зачета
по учебной дисциплине

ОП.05 Основы информационной безопасности

по специальности

09.02.11. Разработка и управление программным обеспечением

РАССМОТРЕН И СОГЛАСОВАН

методической комиссией программирования и компьютерных дисциплин

Протокол № 10 от «15» мая 2025 г.

Председатель методической
комиссии

_____ / Сердюк С. А.
(подпись) (Ф.И.О.)

Разработан на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности
09.02.011 Разработка и управление программным обеспечением

УТВЕРЖДЕН
заместителем директора

_____ / Захаров В. В.
(подпись, Ф.И.О.)

Составители:

Лызлов Максим Сергеевич, преподаватель Колледжа ФГБОУ ВО «ЛГУ им. В. Даля»

I. Паспорт комплекта контрольно-оценочных средств

1.1. Результаты освоения программы учебной дисциплины, подлежащие проверке

1.1.1. Вид профессиональной деятельности

В результате освоения учебной дисциплины ОП.05 Основы информационной безопасности, обучающийся должен обладать предусмотренными ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением профессиональными и общими компетенциями:

Профессиональные компетенции (должны быть сформированы в полном объеме)	**Показатели оценки результата**
ПК 1.5 Защищать информацию в базе данных с использованием технологии защиты информации.	- Реализованы механизмы защиты данных в базе данных (например, шифрование, управление доступом, защита от SQL-инъекций). - Применены технологии защиты информации (например, использование SSL/TLS, хеширование паролей, настройка ролевого доступа). - Проведена проверка безопасности базы данных с использованием инструментов аудита (например, SQLMap, OWASP ZAP). - Составлена документация по реализованным мерам защиты, соответствующая стандартам информационной безопасности.

Общие компетенции (возможна частичная сформированность)	**Показатели оценки результата**
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	- Составлен план профессионального и личностного развития на период практики (например, изучение новых технологий, участие в проектах). - Демонстрация навыков применения правовой и финансовой грамотности (например, понимание лицензий ПО, основ составления сметы на проект). - Участие в профессиональных задачах с учетом инициативности и самостоятельности. - Отражение в отчетах или дневнике практики целей и результатов саморазвития.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом	- Соблюдение этических норм и стандартов антикоррупционного поведения в процессе выполнения задач практики. - Демонстрация уважительного отношения к коллегам и руководителям, независимо от их национальной или религиозной принадлежности. - Участие в профессиональной деятельности с учетом принципов социальной ответственности.

гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.	- Отсутствие нарушений, связанных с профессиональной этикой, подтвержденное обратной связью от руководителя практики.
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	- Успешное использование профессиональной документации на русском языке (например, технических заданий, стандартов). - Работа с документацией на иностранном языке (например, англоязычные мануалы, документация фреймворков или библиотек). - Корректный перевод и интерпретация профессиональных терминов при выполнении задач. - Включение ссылок на использованную документацию в отчетах по практике.

1.1.2. Дидактические единицы «иметь практический опыт», «уметь», «знать».

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной дисциплины должен:

иметь практический опыт:

ПО1. Использовать стандартные методы защиты объектов базы данных.

уметь:

У1. выполнять установку и настройку программного обеспечения для обеспечения работы пользователя с базой данных;

У2. обеспечивать информационную безопасность на уровне базы данных;

У3. определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию;

У4. определять и выстраивать траектории профессионального развития и самообразования;

У5. выявлять достоинства и недостатки коммерческой идеи;

У6. презентовать идеи открытия собственного дела в профессиональной деятельности;

У7. оформлять бизнес-план;

У8. рассчитывать размеры выплат по процентным ставкам кредитования;

У9. определять инвестиционную привлекательность;

У10. презентовать бизнес-идею;

У11. определять источники финансирования коммерческих идей в рамках профессиональной деятельности;

У12. описывать значимость своей специальности;

У13. понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы;

У14. участвовать в диалогах на знакомые общие и профессиональные темы;

У15. строить простые высказывания о себе и о своей профессиональной деятельности;

У16. кратко обосновывать и объяснить свои действия (текущие и планируемые);

У17. писать простые связные сообщения на знакомые или интересующие профессиональные темы

знать:

З1. методы организации целостности данных;

З2. способы контроля доступа к данным и управления привилегиями;

З3. основы разработки приложений баз данных;

З4. основные методы и средства защиты данных в базе данных;

З5. содержание актуальной нормативно-правовой документации;

З6. современная научная и профессиональная терминология;

З7. возможные траектории профессионального развития и самообразования;

З8. основы предпринимательской деятельности;

З9. основы финансовой грамотности;

З10. Правила разработки бизнес-планов;

З11. порядок выстраивания презентации;

кредитные банковские продукты;

З12. сущность гражданско-патриотической позиции, общечеловеческих ценностей;

З13. значимость профессиональной деятельности по специальности;

З14. правила построения простых и сложных предложений на профессиональные темы;

З15. основные общеупотребительные глаголы (бытовая и профессиональная лексика);

З16. лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности;

З17. особенности произношения;

З18. правила чтения текстов профессиональной направленности;

Оценивание уровня освоения учебной дисциплины

2.1. Формы и методы оценивания

Предметом оценивания служат умения и знания, предусмотренные ФГОС СПО по дисциплине ОП.05 Основы информационной безопасности, направленные на формирование общих и профессиональных компетенций. Промежуточная аттестация по учебной дисциплине проводится в форме: опроса, теста, реферата (подготовка информационного сообщения), лабораторных работ, контрольных работ (для текущего контроля), практических занятий, дифференцированного зачета.

2.2. Задания для оценивания уровня учебной дисциплины

Задания для проведения как текущего контроля так и промежуточной аттестации по ОП.05 Основы информационной безопасности, предназначены для проверки результатов освоения умений и усвоения знаний, а также направлены на формирование профессиональных и общих компетенций в соответствии с программой учебной дисциплины.

2.2.1 Регламент проведения и оценивание устного (письменного) опроса

В целях закрепления практического материала и углубления теоретических знаний по разделам теоретического курса ОП.05 предполагается выполнение устных (письменных) опросов студентов, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемой учебной дисциплины.

Критерии оценки устного (письменного) опроса

Оценка	Критерии оценивания
5 баллов	Ответ на вопрос раскрыт полностью, в представленном ответе обоснованно получен правильный ответ.
4 балла	Ответ дан полностью, но нет достаточного обоснования или при верном ответе допущена незначительная ошибка, не влияющая на правильную последовательность рассуждений.
3 балла	Ответы даны частично.
2 балла	Ответ неверен или отсутствует.

2.3.2 Регламент проведения и оценивание рефератов

В целях закрепления и углубления теоретических материала по разделам теоретического курса ОП.05 предполагается выполнение рефератов студентами, что позволяет углубить процесс познания, раскрать творческий потенциал, выработать умения пользоваться научной и специальной литературой, анализировать ее, обобщать и делать выводы, а также выработать умения самостоятельно осваивать некоторые темы учебной дисциплины

.

Критерии оценки устного опроса

Оценка	Критерии оценивания
5 баллов	Ответ по теме раскрыт полностью, выполнены все требования к содержанию и оформлению реферата.
4 балла	Основные требования к реферату выполнены, но при этом допущены недочеты (имеются неточности в изложении материала; не выдержан объем реферата; имеются упущения в оформлении)
3 балла	Имеются существенные отступления от требований к реферированию (тема раскрыта лишь частично; отсутствует логическая последовательность в суждениях; допущены ошибки в оформлении реферата)
2 балла	Требования к реферату не выполнены: тема не раскрыта, правила оформления не соблюдены.

2.3.3 Регламент проведения и оценивание тестирования студентов

В целях закрепления практического материала и углубления теоретических знаний по разделам теоретического курса ОП.05 Основы информационной безопасности предполагается выполнение тестирования студентов, что позволяет углубить процесс познания, раскрыть понимание прикладной значимости осваиваемого учебной дисциплины.

Регламент проведения мероприятия

Предлагается пройти тест в электронном варианте или в распечатанном по опеределенной теме (в тесте от 20 вопросов до 50 вопросов).

Критерии оценки тестирования студентов

За верное решение каждого задания выставляется– 1 балл.

За неверное решение выставляется – 0 баллов.

Шкала оценки тестов

Процент результативности (правильных ответов)	Оценка уровня подготовки	
	балл (отметка)	вербальный аналог
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	неудовлетворительно

2.3.4 Регламент проведения и оценивание практических занятий

В ходе практической работы обучающиеся приобретают умения, предусмотренные рабочей программой учебной дисциплины, учатся самостоятельно работать с оборудованием лаборатории, проводить эксперименты, анализировать полученные результаты и делать выводы, подтверждать теоретические положения лабораторным экспериментом.

Содержание, этапы проведения конкретной практической работы представлены в методических указаниях по проведению практических занятий.

При оценивании практических занятий обучающегося учитывается следующее:

- качество выполнения работы;
- качество оформления отчета по работе;
- качество устных ответов на контрольные вопросы при защите работы.

Критерии оценки практических работ

Оценка	Критерии оценивания
5 баллов	Практическая работа выполнена с соблюдением правил техники безопасности; протокол практической работы оформлен во время занятия, содержит подробное описание всех этапов практической работы. Задание выполнено полностью, в представленном отчете обоснованно получено правильное выполненное задание.
4 балла	Практическая работа выполнена с соблюдением правил техники безопасности; протокол практической работы оформлен во время занятия; этапы практической работы описаны недостаточно подробно. Задание выполнено полностью, но нет достаточного обоснования или при верном решении допущена незначительная ошибка, не влияющая на правильную последовательность рассуждений.
3 балла	Практическая работа выполнена с соблюдением правил техники безопасности; протокол практической работы оформлен во время занятия; но в нем отсутствует описание некоторых этапов практической работы. Задания выполнены частично.
2 балла	Практическая работа выполнена с соблюдением правил техники безопасности; протокол практической работы не оформлен во время занятия или содержит грубые ошибки в оформлении и выполнении. Задание не выполнено.

Защита практической работы - средство контроля, организованное как специальная беседа преподавателя с обучающимся по теме выполняемой практической работы и рассчитанное на выяснение объема знаний и умений обучающегося по конкретной теме.

2.3.5 Регламент проведения и оценивание контрольных работ

Контрольная работа проводится с целью контроля усвоенных умений и знаний и последующего анализа типичных ошибок и затруднений обучающихся в конце изучения раздела/темы.

Письменная контрольная работа включает ХХ вариантов заданий. Задания дифференцируются по уровню сложности. Варианты письменной контрольной работы равноценны по трудности, одинаковы по структуре, параллельны по расположению заданий: под одним и тем же порядковым номером во всех вариантах письменной проверочной работы находится задание, проверяющее один и тот же элемент содержания.

На выполнение контрольной работы отводится **ХХ** минут.

Критерии оценки

«Отлично» - за глубокое и полное овладение содержанием учебного материала, в котором обучающийся свободно и уверенно ориентируется; научно-понятийным аппаратом; за умение практически применять теоретические знания, высказывать и обосновывать свои суждения. Оценка «отлично» предполагает грамотное и логичное изложение ответа, обоснование собственного высказывания с точки зрения известных теоретических положений.

«Хорошо» - обучающийся полно освоил учебный материал, владеет научно-понятийным аппаратом, ориентируется в изученном материале, осознанно применяет теоретические знания на практике, грамотно излагает ответ, но содержание и форма ответа имеют отдельные неточности.

«Удовлетворительно» - обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении теоретических знаний при ответе на практико-ориентированные вопросы; не умеет доказательно обосновать собственные суждения.

«Неудовлетворительно» - обучающийся имеет разрозненные, бессистемные знания по разделу/теме, допускает ошибки в определении базовых понятий, искажает их смысл; не может практически применять теоретические знания.

Критерии оценки

Оценка **«отлично»** выставляется в том случае, если:

- содержание работы соответствует выбранной теме работы;
- работа актуальна, выполнена самостоятельно, имеет творческий характер, отличается определенной новизной;
- дан обстоятельный анализ степени теоретического исследования проблемы, различных подходов к ее решению;
- показано знание нормативной базы, учтены последние изменения в законодательстве и нормативных документах по данной проблеме;
- проблема раскрыта глубоко и всесторонне, материал изложен логично;
- теоретические положения органично сопряжены с практикой; даны представляющие интерес практические рекомендации, вытекающие из анализа проблемы;
- в работе широко используются материалы исследования, проведенного автором самостоятельно или в составе группы (в отдельных случаях допускается опора на вторичный анализ имеющихся данных);
- в работе проведен количественный анализ проблемы, который подкрепляет теорию и иллюстрирует реальную ситуацию, приведены таблицы сравнений, графики, диаграммы, формулы, показывающие умение автора формализовать результаты исследования;

- широко представлена библиография по теме работы;

- приложения к работе иллюстрируют достижения автора и подкрепляют его выводы;

- по своему содержанию и форме работа соответствует всем предъявленным требованиям.

Оценка **«хорошо»** выставляется в том случае, если:

- тема соответствует специальности;

- содержание работы в целом соответствует заданию;

- работа актуальна, написана самостоятельно;

- дан анализ степени теоретического исследования проблемы;

- основные положения работы раскрыты на достаточном теоретическом и методологическом уровне;

- теоретические положения сопряжены с практикой;

- представлены количественные показатели, характеризующие проблемную ситуацию;

- практические рекомендации обоснованы;

- приложения грамотно составлены и прослеживается связь с положениями курсовой работы;

- составлена библиография по теме работы.

Оценка **«удовлетворительно»** выставляется в том случае, если:

- работа соответствует специальности;

- имеет место определенное несоответствие содержания работы заявленной теме;

- исследуемая проблема в основном раскрыта, но не отличается новизной, теоретической глубиной и аргументированностью;

- нарушена логика изложения материала, задачи раскрыты не полностью;

- в работе не полностью использованы необходимые для раскрытия темы научная литература, нормативные документы, а также материалы исследований;

- теоретические положения слабо увязаны с управленческой практикой, практические рекомендации носят формальный бездоказательный характер;

- содержание приложений не освещает решения поставленных задач.

Оценка **«неудовлетворительно»** выставляется в том случае, если:

- тема работы не соответствует специальности;

- содержание работы не соответствует теме;

- работа содержит существенные теоретико-методологические ошибки и поверхностную аргументацию основных положений;

- курсовая работа носит умозрительный и (или) компилятивный характер;

- предложения автора четко не сформулированы.

Оценка за курсовую работу по результатам защиты выставляется в ведомость и зачетную книжку (неудовлетворительная оценка - только в ведомость) за подписью руководителя.

2.3.7 Регламент проведения и оценивание промежуточной аттестации в виде дифференцированного зачета

К дифференцированному зачету по учебной дисциплине допускаются студенты, не имеющие задолженностей по выполненным практическим занятиям и по итогам усвоения материала курса средняя оценка не ниже «удовлетворительно».

Контроль и оценивание уровня освоения учебной дисциплины по темам (разделам)

Элемент учебной дисциплины	**Формы и методы контроля**			
	Текущий контроль		**Промежуточная аттестация**	
	Форма контроля	**Проверяемые ОК, У, З**	**Форма контроля**	**Проверяемые ОК, У, З**
Раздел 1. Теоретические основы информационной безопасности				
Тема 1.1. Основные понятия и задачи информационной безопасности	Устный опрос Самостоятельная работа	*У1-У17;* *З1-З18;* *ОК3,ОК6,* *ОК9;*		
Тема 1.2. Основы защиты информации	Устный опрос Самостоятельная работа Практическая работа №1 Практическая работа №2 Практическая работа №3	*У1-У17;* *З1-З18;* *ОК3,ОК6,* *ОК9;*		
Тема 1.3. Угрозы безопасности защищаемой информации.	Устный опрос Самостоятельная работа Практическая работа №4 Практическая работа №5	*У1-У17;* *З1-З18;* *ОК3,ОК6,* *ОК9;*		

Раздел 2. Методология защиты информации				
Тема 2.1. Методологические подходы к защите информации	Устный опрос Самостоятельная работа	*У1-У17;* *З1-З18;* *ОК3,ОК6,* *ОК9;*		
Тема 2.2. Нормативно правовое регулирование защиты информации	Устный опрос Самостоятельная работа Практическая работа №7 Практическая работа №8 Практическая работа №9	*У1-У17;* *З1-З18;* *ОК3,ОК6,* *ОК9;*		
Тема 2.3. Защита информации в автоматизированных (информационных) системах	Устный опрос Самостоятельная работа Практическая работа №10 Практическая работа №11 Практическая работа №12	*У1-У17;* *З1-З18;* *ОК3,ОК6,* *ОК9;*		
Промежуточная аттестация			Дифференцированный зачет	*У1-У17;* *З1-З18;* *ОК3,ОК6,* *ОК9;*

III. Задания для оценки освоения учебной дисциплины

3.1. Задания для текущего контроля

(прилагаются задания для текущего контроля в соответствии с таблицей 1 данного документа)

Контроль и оценка этих дидактических единиц осуществляются с использованием следующих форм и методов: мониторинга деятельности студента в ходе выполнения практических работ, сдача практических работ, лабораторных работ, устные ответы по теоретическим вопросам, оформление и защита отчета.

3.2. Задания для промежуточной аттестации

(прилагаются задания для промежуточной аттестации)

.

IV. Контрольно-оценочные материалы для дифференцированного зачета

4.1. Общие положения

Дифференцированный зачет предназначен для контроля и оценки результатов освоения учебной дисциплины

ОП.05 Основы информационной безопасности

(код и название учебной дисциплины)

по специальности

09.02.11 Компьютерные системы и комплексы

(код и наименование специальности)

Дифференцированный зачет проводится непосредственно после завершения освоения программы учебной дисциплины. Дифференцированный зачет представляет собой форму независимой оценки результатов обучения.

Дифференцированный зачет носит комплексный практико-ориентированный характер.

Итогом дифференцированного зачета является однозначное решение «вид профессиональной деятельности освоен/не освоен».

При выставлении оценки учитывается роль оцениваемых показателей для выполнения вида профессиональной деятельности, освоение которого проверяется. При отрицательном заключении хотя бы по одному показателю оценки результата освоения профессиональных компетенций принимается решение «вид профессиональной деятельности не освоен». При наличии противоречивых оценок по одному и тому же показателю при выполнении разных видов работ, решение принимается в пользу обучающегося.

4.2. Задания для дифференцированного зачета

Оценка качества подготовки обучающихся по учебной дисциплине ОП.05 Основы информационной безопасности осуществляется в ходе дифференцированного зачета.

Дифференцированный зачет проводится в виде предоставления обучающимся ответов на задание. Задание содержит тестовых задания, вопросы охватывают все разделы рабочей программы (теоретические основы, методология защиты информации) и проверяют компетенции ПК 1.5, ОК 03, ОК 06, ОК 09.

Условием положительной аттестации (вид профессиональной деятельности освоен) на дифференцированном зачете является положительная оценка освоения всех профессиональных компетенций по всем контролируемым показателям.

4.3. Критерии оценивания

Критерии оценки знания теоретического материала:

- оценка «отлично» - отвечает полно, обоснованно, даёт правильные формулировки, точные определения понятий и терминов, полное понимание материала, свободно владеет речью;

- оценка «хорошо» - отвечает полно, обоснованно, но имеет единичные ошибки, которые сам же исправляет после замечания преподавателя, полное понимание материала, свободно владеет речью;

- оценка «удовлетворительно» - ответ не имеет теоретического обоснования, не полное понимание материала, допускает неточности в формулировках, определениях понятий и терминов, иногда искажает смысл;

- оценка «неудовлетворительно» - ответ не имеет теоретического обоснования, не даёт правильных формулировок, определений понятий и терминов, полное непонимание материала

Критерии оценки практических умений:

- оценка «отлично» выставляется обучающемуся, демонстрирующему всестороннее систематическое знание учебного материала, умение свободно выполнять практические задания, максимально приближенные к будущей профессиональной деятельности в стандартных и нестандартных ситуациях, освоившему основную литературу и знакомому с дополнительной литературой, усвоившему взаимосвязь основных понятий и их значении для приобретаемой специальности;

- оценка «хорошо» выставляется обучающемуся, демонстрирующему полное знание учебного материала, успешно выполнившему практические

задания, максимально приближенные к будущей профессиональной деятельности в стандартных ситуациях, освоившему основную рекомендованную литературу, показавшему систематический характер знаний по междисциплинарным курсам, способному к их самостоятельному пополнению и обновлению в ходе дальнейшей учёбы и профессиональной деятельности. Содержание и форма ответа имеют отдельные неточности;

- оценка «удовлетворительно» выставляется обучающемуся, демонстрирующему знание основного учебного материала в объёме, необходимом для дальнейшей учёбы и предстоящей работы по специальности, справляющемуся с выполнением заданий, предусмотренных рабочей программой, обладающему необходимыми знаниями, но допустившему неточности в определении понятий, в применении знаний для решения профессиональных задач, в неумении обосновывать свои рассуждения.

- оценка «неудовлетворительно» выставляется обучающемуся, демонстрирующему отсутствие знаний основного учебного материала в объёме, необходимом для дальнейшей учёбы и предстоящей работы по специальности, не справляющемуся с выполнением заданий, предусмотренных рабочей программой, не обладающему необходимыми знаниями, допустившему грубые неточности в определении понятий, в применении знаний для решения профессиональных задач, в неумении обосновывать свои рассуждения

Критерии оценки дифференцированного зачета

Оценка «отлично» выставляется студенту за глубокое и полное овладение содержанием учебного материала, в котором студент легко ориентируется, за владение понятийным аппаратом за умение связывать теорию с практикой, высказывать и обосновывать свои суждения. Работа выполнена грамотно, ответы на теоретические вопросы изложены грамотно и логично. Практические задания выполнены полностью и получен верный ответ.

Оценка «хорошо» выставляется студенту, если студент полно освоил учебный материал, владеет понятийным аппаратом, ориентируется в изученном материале, осознанно применяет знания для решения практических задач, грамотно излагает ответ, но содержание и форма ответа имеют некоторые неточности. Практические задания выполнены полностью, но при выполнении обнаружились недостатки.

Оценка «удовлетворительно» выставляется студенту, если студент демонстрирует знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических задач, не умеет

доказательно обосновать свои суждения. Практические задания выполнены не полностью, но студент владеет основными навыками.

Оценка «неудовлетворительно» выставляется студенту, если студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определение понятий, искажает их смысл, беспорядочно и неуверенно излагает материал, не может применять знания для решения практической задачи; работа показала полное отсутствие у студентов обязательных знаний и навыков.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ВЛАДИМИРА ДАЛЯ»

КОЛЛЕДЖ

Рассмотрено и утверждено
на заседании методической комиссии
_____
Протокол от «__» _____ 20__ года № ___
Председатель комиссии
_____ С.А. Сердюк

УТВЕРЖДАЮ
Заместитель директора
_____ В.В. Захаров
«__» _____ 20__ г.

КОМПЛЕКТ ЗАДАНИЙ
для проведения промежуточной аттестации
в форме дифференцированного зачета

по учебной дисциплине

ОП.05 Основы информационной безопасности

по специальности
09.02.11 Разработка и управление программным обеспечением

для студентов ___ курса _____группы _____

формы обучения __очная_____

Преподаватель: _____ М.С. Лызлов
(подпись)

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ

По учебной дисциплине ОП.05 Основы информационной безопасности, по специальности 09.02.11 Разработка и управление программным обеспечением

Вариант 1

1. Что такое информационная безопасность? (1 правильный ответ)

a) Процесс разработки программного обеспечения
b) Защита информации от несанкционированного доступа, использования, раскрытия, искажения, уничтожения
c) Управление базами данных
d) Создание резервных копий данных

2. Какие основные составляющие информационной безопасности? (1 правильный ответ)

a) Скорость, объем, качество
b) Надежность, совместимость, производительность
c) Конфиденциальность, целостность, доступность
d) Доступность, масштабируемость, безопасность

3. Какое место занимает информационная безопасность в системе национальной безопасности? (1 правильный ответ)

a) Регулирует экономическую политику
b) Контролирует транспортную систему
c) Обеспечивает защиту государственных интересов в информационной сфере
d) Управляет образовательными процессами

4. Какие виды защищаемой информации существуют? (Несколько правильных ответов)

a) Персональные данные
b) Публичные отчеты
c) Коммерческая тайна
d) Рекламные материалы

5. Какие основные источники угроз информационной безопасности? (Несколько правильных ответов)

a) Хакеры
b) Вирусы
c) Законодательные акты
d) Внутренние сотрудники

6. Что такое риск информационной безопасности? (1 правильный ответ)

a) Скорость обработки данных
b) Объем хранимой информации
c) Уровень защиты информации
d) Вероятность реализации угрозы с негативными последствиями

7. Какие этапы входят в жизненный цикл информации? (1 правильный ответ)
a) Разработка, тестирование, внедрение
b) Создание, обработка, передача, хранение, уничтожение
c) Планирование, исполнение, контроль
d) Анализ, проектирование, реализация

8. В чем различие между конфиденциальностью и целостностью информации? (1 правильный ответ)
a) Конфиденциальность регулирует хранение, целостность — доступность
b) Конфиденциальность защищает от вирусов, целостность — от хакеров
c) Конфиденциальность предотвращает несанкционированный доступ, целостность обеспечивает неизменность данных
d) Конфиденциальность обеспечивает скорость передачи, целостность — объем данных

9. Что подразумевается под доступностью информации? (1 правильный ответ)
a) Шифрование данных
b) Хранение данных на сервере
c) Возможность своевременного доступа для авторизованных пользователей
d) Уничтожение устаревшей информации

10. Как классифицируется информация по видам тайны? (Несколько правильных ответов)
a) Государственная
b) Техническая
c) Коммерческая
d) Персональная

11. Какие степени конфиденциальности существуют для защищаемой информации? (1 правильный ответ)
a) Высокая, средняя, низкая
b) Совершенно секретно, секретно, для служебного пользования
c) Публичная, ограниченная, закрытая
d) Основная, дополнительная, вспомогательная

12. Какое из перечисленных является примером преступления в сфере информационных технологий? (1 правильный ответ)
a) Нарушение трудового законодательства
b) Несанкционированный доступ к компьютерной информации
c) Нарушение правил дорожного движения
d) Несоблюдение налогового законодательства

13. Какова цель политики информационной безопасности? (1 правильный ответ)
a) Разработка программного обеспечения
b) Управление финансовыми потоками
c) Обучение сотрудников программированию
d) Определение правил и процедур защиты информации

14. Какова роль менеджмента информационной безопасности в организации? (1 правильный ответ)
a) Разработка маркетинговых стратегий
b) Координация процессов защиты информации
c) Управление производственными процессами
d) Контроль качества продукции

15. Что такое уязвимость в контексте информационной безопасности? (1 правильный ответ)
a) Программное обеспечение для защиты данных
b) Законодательный акт
c) Слабое место в системе, которое может быть использовано для атаки
d) Сертификат безопасности

16. Какие методы используются для оценки уязвимостей? (Несколько правильных ответов)
a) Сканирование уязвимостей
b) Тестирование на проникновение
c) Разработка программ
d) Финансовый аудит

17. Какие каналы несанкционированного доступа к информации существуют? (Несколько правильных ответов)
a) Сетевые атаки
b) Физический доступ
c) Обучение сотрудников
d) Социальная инженерия

18. Как классифицировать угрозы информационной безопасности по их источникам? (1 правильный ответ)
a) Технические, программные, аппаратные
b) Внешние, внутренние, случайные
c) Финансовые, юридические, административные
d) Плановые, внеплановые, периодические

19. Какие меры противодействия угрозам информационной безопасности существуют? (Несколько правильных ответов)
a) Антивирусное программное обеспечение
b) Межсетевые экраны
c) Маркетинговая стратегия
d) Шифрование данных

20. Какова цель нормативно-правового регулирования в области информационной безопасности? (1 правильный ответ)
a) Регулирование трудовых отношений
b) Установление правил защиты информации
c) Контроль качества продукции
d) Управление образовательными процессами

21. Какой российский законодательный акт регулирует защиту информации? (1 правильный ответ)
a) Трудовой кодекс РФ
b) Федеральный закон «Об информации, информационных технологиях и о защите информации»
c) Гражданский кодекс РФ
d) Налоговый кодекс РФ

22. Какие международные стандарты определяют требования к защите информации? (Несколько правильных ответов)
a) ISO/IEC 27001
b) ISO 9001
c) ISO/IEC 27002
d) IEEE 802.11

23. Что такое система сертификации в области защиты информации в РФ? (1 правильный ответ)
a) Процесс разработки программного обеспечения
b) Процесс подтверждения соответствия средств защиты стандартам
c) Процедура финансового аудита
d) Система обучения персонала

24. Какие механизмы защиты информации применяются в автоматизированных системах? (Несколько правильных ответов)
a) Аутентификация
b) Шифрование
c) Разработка кода
d) Контроль доступа

25. Какие программно-аппаратные средства защиты информации существуют? (Несколько правильных ответов)
a) Межсетевые экраны
b) Антивирусы
c) Текстовые редакторы
d) Системы обнаружения вторжений

26. Что такое организационно-распорядительная защита информации? (1 правильный ответ)
a) Программное обеспечение для защиты данных
b) Совокупность документов и процедур для защиты информации
c) Физическая охрана объектов
d) Резервное копирование данных

27. Какие принципы лежат в основе организационно-распорядительной системы защиты? (Несколько правильных ответов)
a) Законность
b) Системность
c) Скорость
d) Комплексность

28. Какие факторы воздействуют на информацию в автоматизированных системах? (Несколько правильных ответов)
a) Угрозы
b) Уязвимости
c) Финансовые ограничения
d) Сбои оборудования

29. Что такое государственная тайна? (1 правильный ответ)
a) Публичные данные правительства
b) Информация, защищаемая государством от разглашения
c) Финансовые отчеты государства
d) Образовательные материалы

30. Какие методы анализа рисков информационной безопасности существуют? (Несколько правильных ответов)
a) Анализ рисков
b) Моделирование угроз
c) Финансовый аудит
d) Тестирование на проникновение

Вариант 2

1. Что такое информация в контексте информационной безопасности? (1 правильный ответ)

a) Финансовые отчеты организации
b) Рекламные материалы
c) Данные, подлежащие защите от несанкционированного доступа
d) Программное обеспечение для управления базами данных

2. Какие объекты входят в состав защищаемых систем? (Несколько правильных ответов)

a) Информационные системы
b) Транспортные средства
c) Базы данных
d) Серверы

3. Как информационная безопасность связана с национальной безопасностью? (1 правильный ответ)

a) Регулирует экономические процессы
b) Контролирует транспортную инфраструктуру
c) Управляет образовательной системой
d) Защищает государственные интересы в информационной сфере

4. Какие носители защищаемой информации существуют? (Несколько правильных ответов)

a) Жесткие диски
b) Бумажные документы
c) Рекламные буклеты
d) Флеш-накопители

5. Какие факторы воздействуют на информацию в автоматизированных системах? (Несколько правильных ответов)

a) Финансовые ограничения
b) Угрозы
c) Уязвимости
d) Сбои оборудования

6. Что такое угроза информации? (1 правильный ответ)

a) Законодательный акт
b) Потенциальное событие, способное нанести ущерб информации
c) Программное обеспечение для защиты данных
d) Сертификат безопасности

7. Какие этапы включает жизненный цикл конфиденциальной информации? (1 правильный ответ)

a) Планирование, тестирование, внедрение
b) Анализ, проектирование, реализация
c) Создание, обработка, передача, хранение, уничтожение
d) Разработка, контроль, аудит

8. В чем заключается сущность целостности информации? (1 правильный ответ)
a) Сохранение данных на сервере
b) Обеспечение неизменности и достоверности данных
c) Уничтожение устаревших данных
d) Шифрование информации

9. Как обеспечивается конфиденциальность информации? (1 правильный ответ)
a) Увеличением скорости передачи данных
b) Резервным копированием
c) Ограничением доступа для неавторизованных лиц
d) Анализом уязвимостей

10. Какие степени секретности существуют для информации? (1 правильный ответ)
a) Высокая, средняя, низкая
b) Публичная, ограниченная, закрытая
c) Совершенно секретно, секретно, для служебного пользования
d) Техническая, финансовая, юридическая

11. Что такое государственная тайна? (1 правильный ответ)
a) Публичные данные правительства
b) Финансовые отчеты государства
c) Образовательные материалы
d) Информация, защищаемая государством от разглашения

12. Какое из перечисленных является примером информационного преступления? (1 правильный ответ)
a) Нарушение трудового законодательства
b) Нарушение экологических норм
c) Хакерская атака на сервер
d) Несоблюдение налоговых правил

13. Какова роль политики информационной безопасности в организации? (1 правильный ответ)
a) Управление персоналом
b) Контроль финансов
c) Определение процедур защиты информации
d) Разработка маркетинговых стратегий

14. Какова модель интеграции информационной безопасности в деятельность организации? (1 правильный ответ)
a) Разработка программного обеспечения
b) Проведение финансового аудита
c) Включение процессов защиты в основные бизнес-процессы
d) Обучение сотрудников продажам

15. Что такое уязвимость информации? (1 правильный ответ)
a) Законодательный акт
b) Сертификат безопасности
c) Программное обеспечение для защиты
d) Слабое место, которое может быть использовано для атаки

16. Какие методы оценки уязвимостей существуют? (Несколько правильных ответов)
a) Финансовый аудит
b) Анализ рисков
c) Тестирование на проникновение
d) Разработка кода

17. Какие каналы несанкционированного доступа к информации существуют? (Несколько правильных ответов)
a) Резервное копирование
b) Сетевые атаки
c) Социальная инженерия
d) Физический доступ

18. Как классифицировать угрозы по их системным характеристикам? (1 правильный ответ)
a) Финансовые, юридические, административные
b) Внешние, внутренние, случайные
c) Технические, программные, аппаратные
d) Плановые, внеплановые, периодические

19. Какие меры предотвращения угроз информационной безопасности существуют? (Несколько правильных ответов)
a) Разработка маркетинговых стратегий
b) Антивирусное ПО
c) Межсетевые экраны
d) Шифрование

20. Что регулируют нормативные акты в области защиты информации? (1 правильный ответ)
a) Трудовые отношения
b) Правила и процедуры защиты информации
c) Производственные процессы
d) Образовательные программы

21. Какой международный стандарт применяется в области информационной безопасности? (1 правильный ответ)
a) ISO 9001
b) IEEE 802.11
c) ISO/IEC 27001
d) ISO 14001

22. Какие документы входят в систему сертификации РФ по защите информации? (Несколько правильных ответов)
a) Нормативные акты
b) Финансовые отчеты
c) Стандарты
d) Сертификаты соответствия

23. Какие программные средства используются для защиты информации? (Несколько правильных ответов)
a) Текстовые редакторы
b) Антивирусы
c) Системы обнаружения вторжений
d) Браузеры

24. Какие меры защиты реализуются в автоматизированных системах? (Несколько правильных ответов)
a) Аутентификация
b) Шифрование
c) Планирование
d) Контроль доступа

25. Что такое инженерно-техническая защита объектов информатизации? (1 правильный ответ)
a) Программное обеспечение для защиты данных
b) Резервное копирование
c) Физическая защита объектов и оборудования
d) Обучение персонала

26. Какие принципы работы с кадрами применяются для обеспечения информационной безопасности? (Несколько правильных ответов)
a) Обучение
b) Контроль
c) Разработка программ
d) Проверка персонала

27. Какие элементы включает процесс менеджмента информационной безопасности? (Несколько правильных ответов)
a) Планирование
b) Реализация
c) Финансовый аудит
d) Корректировка

28. Какие российские стандарты регулируют защиту информации? (1 правильный ответ)
a) ГОСТ Р ИСО 9001
b) ГОСТ Р ИСО/МЭК 27001
c) ГОСТ Р 52001
d) ГОСТ Р 14001

29. Что такое конфиденциальная информация? (1 правильный ответ)
a) Публичные данные
b) Информация, доступ к которой ограничен
c) Финансовые отчеты
d) Учебные материалы

30. Какие методы анализа угроз информационной безопасности существуют? (Несколько правильных ответов)
a) Моделирование угроз
b) Финансовый аудит
c) Анализ рисков
d) Тестирование на проникновение

Вариант 3

1. Что такое информационные процессы в контексте информационной безопасности? (1 правильный ответ)

a) Процессы разработки программного обеспечения
b) Процессы создания, обработки, передачи и хранения информации
c) Процессы финансового учета
d) Процессы маркетингового анализа

2. Какие основные задачи информационной безопасности? (Несколько правильных ответов)

a) Обеспечение конфиденциальности
b) Увеличение скорости обработки данных
c) Обеспечение целостности
d) Обеспечение доступности

3. Как информационная безопасность влияет на национальную безопасность? (1 правильный ответ)

a) Регулирует экономические процессы
b) Контролирует транспортную систему
c) Защищает государственные интересы в информационной сфере
d) Управляет образовательной системой

4. Какие виды защищаемой информации существуют? (Несколько правильных ответов)

a) Персональные данные
b) Публичные новости
c) Государственная тайна
d) Коммерческая тайна

5. Какие источники угроз информационной безопасности существуют? (Несколько правильных ответов)

a) Хакеры
b) Вирусы
c) Законодательные акты
d) Внутренние сотрудники

6. Что такое риск информационной безопасности? (1 правильный ответ)

a) Уровень защиты информации
b) Скорость обработки данных
c) Вероятность реализации угрозы с негативными последствиями
d) Объем хранимой информации

7. Какие этапы включает жизненный цикл информации ограниченного доступа? (1 правильный ответ)

a) Планирование, тестирование, внедрение
b) Анализ, проектирование, реализация
c) Разработка, контроль, аудит
d) Создание, обработка, передача, хранение, уничтожение

8. В чем заключается принцип доступности информации? (1 правильный ответ)
a) Хранение данных на сервере
b) Уничтожение устаревших данных
c) Обеспечение своевременного доступа для авторизованных пользователей
d) Шифрование информации

9. Что такое конфиденциальная информация? (1 правильный ответ)
a) Публичные данные
b) Финансовые отчеты
c) Информация, доступ к которой ограничен
d) Учебные материалы

10. Как классифицировать информацию по видам тайны? (Несколько правильных ответов)
a) Государственная
b) Техническая
c) Служебная
d) Персональная

11. Какие степени секретности существуют для информации? (1 правильный ответ)
a) Высокая, средняя, низкая
b) Публичная, ограниченная, закрытая
c) Совершенно секретно, секретно, для служебного пользования
d) Техническая, финансовая, юридическая

12. Какое из перечисленных является примером преступления в сфере информации? (1 правильный ответ)
a) Нарушение трудового законодательства
b) Нарушение экологических норм
c) Фишинговая атака
d) Несоблюдение налоговых правил

13. Что такое политика информационной безопасности организации? (1 правильный ответ)
a) Программное обеспечение для защиты данных
b) Финансовый отчет
c) Документ, определяющий правила защиты информации
d) Учебная программа

14. Какие элементы включает процесс менеджмента информационной безопасности? (Несколько правильных ответов)
a) Планирование
b) Финансовый аудит
c) Реализация
d) Корректировка

15. Что подразумевается под уязвимостью информации? (1 правильный ответ)
a) Программное обеспечение для защиты
b) Законодательный акт
c) Слабое место, которое может быть использовано для атаки
d) Сертификат безопасности

16. Какие методы используются для анализа угроз информационной безопасности? (Несколько правильных ответов)
a) Анализ рисков
b) Моделирование угроз
c) Разработка кода
d) Тестирование на проникновение

17. Какие методы несанкционированного доступа к информации существуют? (Несколько правильных ответов)
a) Социальная инженерия
b) Сетевые атаки
c) Резервное копирование
d) Физический доступ

18. Как классифицировать угрозы по их воздействию на информацию? (1 правильный ответ)
a) Технические, программные, аппаратные
b) Угрозы конфиденциальности, целостности, доступности
c) Финансовые, юридические, административные
d) Плановые, внеплановые, периодические

19. Какие меры защиты информации существуют? (Несколько правильных ответов)
a) Антивирусное ПО
b) Межсетевые экраны
c) Разработка маркетинговых стратегий
d) Шифрование

20. Какова роль законодательных актов в обеспечении информационной безопасности? (1 правильный ответ)
a) Регулирование трудовых отношений
b) Контроль качества продукции
c) Установление правил защиты информации
d) Управление образовательными процессами

21. Какой российский стандарт регулирует защиту информации? (1 правильный ответ)
a) ГОСТ Р ИСО 9001
b) ГОСТ Р 52001
c) ГОСТ Р ИСО/МЭК 27001
d) ГОСТ Р 14001

22. Что такое сертификация в области информационной безопасности в РФ? (1 правильный ответ)
a) Разработка программного обеспечения
b) Финансовый аудит
c) Подтверждение соответствия средств защиты стандартам
d) Обучение персонала

23. Какие механизмы защиты информации применяются в автоматизированных системах? (Несколько правильных ответов)
a) Аутентификация
b) Шифрование
c) Планирование
d) Контроль доступа

24. Какие программно-аппаратные средства используются для защиты информации? (Несколько правильных ответов)
a) Межсетевые экраны
b) Антивирусы
c) Текстовые редакторы
d) Системы обнаружения вторжений

25. Что такое внутриобъектовый режим в контексте информационной безопасности? (1 правильный ответ)
a) Программное обеспечение для защиты данных
b) Меры контроля доступа на объекте
c) Резервное копирование
d) Обучение персонала

26. Какие принципы лежат в основе организационно-распорядительной защиты? (Несколько правильных ответов)
a) Законность
b) Системность
c) Скорость
d) Комплексность

27. Какие факторы воздействуют на информацию в автоматизированных системах? (Несколько правильных ответов)
a) Угрозы
b) Уязвимости
c) Финансовые ограничения
d) Сбои оборудования

28. Какие носители защищаемой информации существуют? (Несколько правильных ответов)
a) Жесткие диски
b) Бумажные документы
c) Рекламные буклеты
d) Флеш-накопители

29. Что такое государственная тайна? (1 правильный ответ)
a) Публичные данные правительства
b) Финансовые отчеты государства
c) Информация, защищаемая государством от разглашения
d) Образовательные материалы

30. Какие методы анализа рисков информационной безопасности существуют? (Несколько правильных ответов)
a) Анализ рисков
b) Моделирование угроз
c) Финансовый аудит
d) Тестирование на проникновение

Вариант 4

1. Дайте определение информационной безопасности как дисциплины. (1 правильный ответ)

a) Наука о разработке программного обеспечения
b) Наука о финансовом учете
c) Наука о защите информации от несанкционированного доступа и угроз
d) Наука о маркетинговом анализе

2. Какие объекты входят в сферу информационной безопасности? (Несколько правильных ответов)

a) Информационные системы
b) Транспортные средства
c) Базы данных
d) Серверы

3. Как информационная безопасность связана с государственной безопасностью? (1 правильный ответ)

a) Регулирует экономические процессы
b) Контролирует транспортную инфраструктуру
c) Управляет образовательной системой
d) Защищает государственные интересы в информационной сфере

4. Какие источники защищаемой информации существуют? (Несколько правильных ответов)

a) Базы данных
b) Рекламные буклеты
c) Серверы
d) Публичные новости

5. Какие факторы влияют на информацию в автоматизированных системах? (Несколько правильных ответов)

a) Угрозы
b) Уязвимости
c) Финансовые ограничения
d) Сбои оборудования

6. Что такое угроза безопасности информации? (1 правильный ответ)

a) Программное обеспечение для защиты данных
b) Законодательный акт
c) Потенциальное событие, способное нанести ущерб информации
d) Сертификат безопасности

7. Какие этапы включает жизненный цикл конфиденциальной информации? (1 правильный ответ)

a) Планирование, тестирование, внедрение
b) Создание, обработка, передача, хранение, уничтожение
c) Анализ, проектирование, реализация
d) Разработка, контроль, аудит

8. В чем заключается принцип целостности информации? (1 правильный ответ)
a) Сохранение данных на сервере
b) Уничтожение устаревших данных
c) Обеспечение неизменности и достоверности данных
d) Шифрование информации

9. Как обеспечивается доступность информации в системах? (1 правильный ответ)
a) Увеличение скорости передачи данных
b) Своевременный доступ для авторизованных пользователей
c) Резервное копирование
d) Анализ уязвимостей

10. Как классифицировать информацию по степеням конфиденциальности? (1 правильный ответ)
a) Высокая, средняя, низкая
b) Публичная, ограниченная, закрытая
c) Совершенно секретно, секретно, для служебного пользования
d) Техническая, финансовая, юридическая

11. Что такое конфиденциальная информация? (1 правильный ответ)
a) Публичные данные
b) Финансовые отчеты
c) Учебные материалы
d) Информация, доступ к которой ограничен

12. Какое из перечисленных является примером информационного преступления? (1 правильный ответ)
a) Нарушение трудового законодательства
b) Вредоносное ПО
c) Нарушение экологических норм
d) Несоблюдение налоговых правил

13. Какова цель разработки политики информационной безопасности? (1 правильный ответ)
a) Управление персоналом
b) Контроль финансов
c) Определение правил и процедур защиты информации
d) Разработка маркетинговых стратегий

14. Каков процесс интеграции информационной безопасности в организацию? (1 правильный ответ)
a) Разработка программного обеспечения
b) Проведение финансового аудита
c) Включение процессов защиты в основные бизнес-процессы
d) Обучение сотрудников продажам

15. Что такое уязвимость в информационной безопасности? (1 правильный ответ)
a) Программное обеспечение для защиты
b) Законодательный акт
c) Слабое место, которое может быть использовано для атаки
d) Сертификат безопасности

16. Какие методики анализа рисков информационной безопасности существуют? (Несколько правильных ответов)
a) Анализ рисков
b) Моделирование угроз
c) Финансовый аудит
d) Тестирование на проникновение

17. Какие каналы несанкционированного доступа к информации существуют? (Несколько правильных ответов)
a) Сетевые атаки
b) Социальная инженерия
c) Резервное копирование
d) Физический доступ

18. Как классифицировать угрозы по их источникам и типам? (1 правильный ответ)
a) Технические, программные, аппаратные
b) Внешние, внутренние, случайные
c) Финансовые, юридические, административные
d) Плановые, внеплановые, периодические

19. Какие меры противодействия угрозам информационной безопасности существуют? (Несколько правильных ответов)
a) Антивирусное ПО
b) Межсетевые экраны
c) Разработка маркетинговых стратегий
d) Шифрование

20. Какие нормативные акты регулируют защиту информации в РФ? (1 правильный ответ)
a) Трудовой кодекс РФ
b) Гражданский кодекс РФ
c) Федеральный закон «Об информации, информационных технологиях и о защите информации»
d) Налоговый кодекс РФ

21. Какой международный стандарт применяется в области информационной безопасности? (1 правильный ответ)
a) ISO 9001
b) IEEE 802.11
c) ISO/IEC 27001
d) ISO 14001

22. Какие документы входят в систему сертификации РФ по защите информации? (Несколько правильных ответов)
a) Нормативные акты
b) Финансовые отчеты
c) Стандарты
d) Сертификаты соответствия

23. Какие механизмы защиты информации применяются в автоматизированных системах? (Несколько правильных ответов)
a) Аутентификация
b) Шифрование
c) Планирование
d) Контроль доступа

24. Какие программные средства используются для защиты информации? (Несколько правильных ответов)
a) Антивирусы
b) Текстовые редакторы
c) Системы обнаружения вторжений
d) Браузеры

25. Что такое инженерно-техническая защита объектов информатизации? (1 правильный ответ)
a) Программное обеспечение для защиты данных
b) Резервное копирование
c) Физическая защита объектов и оборудования
d) Обучение персонала

26. Какие принципы лежат в основе организационно-распорядительной защиты информации? (Несколько правильных ответов)
a) Законность
b) Системность
c) Скорость
d) Комплексность

27. Какие элементы включает процесс менеджмента информационной безопасности? (Несколько правильных ответов)
a) Планирование
b) Реализация
c) Финансовый аудит
d) Корректировка

28. Какие российские стандарты регулируют защиту информации? (1 правильный ответ)
a) ГОСТ Р ИСО 9001
b) ГОСТ Р 52001
c) ГОСТ Р ИСО/МЭК 27001
d) ГОСТ Р 14001

29. Какие носители защищаемой информации существуют? (Несколько правильных ответов)
a) Жесткие диски
b) Бумажные документы
c) Рекламные буклеты
d) Флеш-накопители

30. Какие методы анализа угроз информационной безопасности существуют? (Несколько правильных ответов)
a) Анализ рисков
b) Моделирование угроз
c) Финансовый аудит
d) Тестирование на проникновение

Вариант 1		Вариант 2		Вариант 3		Вариант 4	
Вопрос	**Правильный ответ**	**Вопрос**	**Правильный ответ**	**Вопрос**	**Правильный ответ**	**Вопрос**	**Правильный ответ**
1	b	1	c	1	b	1	c
2	c	2	a, c, d	2	a, c, d	2	a, c, d
3	c	3	d	3	c	3	d
4	a, c	4	a, b, d	4	a, c, d	4	a, c
5	a, b, d	5	b, c, d	5	a, b, d	5	a, b, d
6	d	6	b	6	c	6	c
7	b	7	c	7	d	7	b
8	c	8	b	8	c	8	c
9	c	9	c	9	c	9	b
10	a, c, d	10	c	10	a, c, d	10	c
11	b	11	d	11	c	11	d
12	b	12	c	12	c	12	b
13	d	13	c	13	c	13	c
14	b	14	c	14	a, c, d	14	c
15	c	15	d	15	c	15	c
16	a, b	16	b, c	16	a, b, d	16	a, b, d
17	a, b, d	17	b, c, d	17	a, b, d	17	a, b, d
18	b	18	b	18	b	18	b
19	a, b, d	19	b, c, d	19	a, b, d	19	a, b, d
20	b	20	b	20	c	20	c
21	b	21	c	21	c	21	c
22	a, c	22	a, c, d	22	c	22	a, c, d
23	b	23	b, c	23	a, b, d	23	a, b, d
24	a, b, d	24	a, b, d	24	a, b, d	24	a, c
25	a, b, d	25	c	25	b	25	c
26	b	26	a, b, d	26	a, b, d	26	a, b, d
27	a, b, d	27	a, b, d	27	a, b, d	27	a, b, d
28	a, b, d	28	b	28	a, b, d	28	c
29	b	29	b	29	c	29	a, b, d
30	a, b, d	30	a, c, d	30	a, b, d	30	a, b, d