МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

И.о. директора института, кандидат технических наук, доцент

А.А. Порохня

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Информационная безопасность
название дисциплины

Направление подготовки	09.03.03 Прикладная информатика
Направленность (профиль)	Прикладная информатика в экономике
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	6

Введение

1. Назначение: ФОС предназначен для объективной оценки уровня сформированности компетенций.

2. ФОС является приложением к программе дисциплины Информационная безопасность

3. Разработчик Орлова А.Ю., доцент департамента цифровых, робототехнических систем и электроники.

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель Азаров И.В., и.о. директора департамента цифровых, робототехнических систем и электроники

Члены комиссии:

Амироков С.Р., доцент департамента цифровых, робототехнических систем и электроники

Орлинская О.Г., доцент департамента цифровых, робототехнических систем и электроники

Представитель организации-работодателя Черевко С.А., генеральный директор ООО "КРАФТКОД"

(*Ф.И.О., должность*)

Экспертное заключение: ФОС по дисциплине позволяет оценить уровень сформированности компетенций. Приступить к апробации.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Уровни сформированности компетенци(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
ОПК-3				
ИД-4. ОПК-3. решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности	С трудом решат стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности	Слабо решат стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности	В целом. решат стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности	решат стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности
ПК-9				
ИД-1 ПК-9 осуществлять ведение базы данных для решения прикладных задач.	С трудом осуществляет ведение базы данных для решения прикладных задач	Слабо осуществляет ведение базы данных для решения прикладных задач	В целом. осуществляет ведение базы данных для решения прикладных задач	осуществляет ведение базы данных для решения прикладных задач
ИД-2 ПК-9 осуществлять поддержку информационного обеспечения для решения прикладных задач.	С трудом осуществляет поддержку информационного обеспечения для решения прикладных задач	Слабо осуществляет поддержку информационного обеспечения для решения прикладных задач	В целом. осуществляет поддержку информационного обеспечения для решения прикладных задач	осуществляет поддержку информационного обеспечения для решения прикладных задач
ПК-10				
ИД-1 ПК-90 принимать участие в организации ИТ-инфраструктуры предприятия.	С трудом принимает участие в организации ИТ-инфраструктуры предприятия.	Слабо принимает участие в организации ИТ-инфраструктуры	В целом. принимает участие в организации ИТ-инфраструктуры	принимает участие в организации ИТ-инфраструктуры
ИД-2 ПК-90 принимать участие в управлении информационной безопасностью предприятия.	С трудом принимает участие в управлении информационной безопасностью предприятия.	Слабо принимает участие в управлении информационной безопасностью предприятия.	В целом. принимает участие в управлении информационной безопасностью предприятия.	принимает участие в управлении информационной безопасностью предприятия.

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения очная, семестр 6	
1.	d	Основные составляющие информационной безопасности: a) Целостность b) Достоверность c) Конфиденциальность d) Все ответы верны	ОПК-3
2.	a	Для чего создаются информационные системы? a)Получения определенных информационных услуг b)Обработки информации c)Все ответы верны	ОПК-3
3.	a	Защита информации – это…? a) Комплекс мероприятий, направленных на обеспечение информационной безопасности b)Процесс разработки структуры базы данных в соответствии с требованиями пользователей c)Небольшая программа для выполнения определенной задачи	ОПК-3
4.	a,c	Где применяются средства контроля динамической целостности? a) Анализе потока финансовых сообщений b) Обработке данных c) При выявлении кражи, дублирования отдельных сообщений	ОПК-3
5.	a	По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы: a)Невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности b)Обрабатывать большой объем программной информации c)Нет правильного ответа	ОПК-3
6.	3	К правовым методам, обеспечивающим информационную безопасность, относятся: 1. Разработка аппаратных средств обеспечения правовых данных 2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий	ОПК-3

		3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности	
7.	2	Основными источниками угроз информационной безопасности являются все указанное в списке: 1. Хищение жестких дисков, подключение к сети, инсайдерство 2. Перехват данных, хищение данных, изменение архитектуры системы 3. Хищение данных, подкуп системных администраторов, нарушение регламента работы	ОПК-3
8.	1	Виды информационной безопасности: 1. Персональная, корпоративная, государственная 2. Клиентская, серверная, сетевая 3. Локальная, глобальная, смешанная	ОПК-3
9.	1	Цели информационной безопасности – своевременное обнаружение, предупреждение: 1. несанкционированного доступа, воздействия в сети 2. инсайдерства в организации 3. чрезвычайных ситуаций	ОПК-3
10.	1	Основные объекты информационной безопасности: 1. Компьютерные сети, базы данных 2 Информационные системы, психологическое состояние пользователей 3. Бизнес-ориентированные, коммерческие системы	ОПК-3
11.	3	Основными рисками информационной безопасности являются: 1. Искажение, уменьшение объема, перекодировка информации 2. Техническое вмешательство, выведение из строя оборудования сети 3. Потеря, искажение, утечка информации	ОПК-3
12.	1	К основным принципам обеспечения информационной безопасности относится: 1. Экономической эффективности системы безопасности 2. Многоплатформенной реализации системы 3. Усиления защищенности всех звеньев системы	ОПК-3
13.	2	Основными субъектами информационной безопасности являются: 1. руководители, менеджеры, администраторы компаний 2. органы права, государства, бизнеса 3. сетевые базы данных, фаерволлы	ОПК-3

14.	1	К основным функциям системы безопасности можно отнести все перечисленное: 1. Установление регламента, аудит системы, выявление рисков 2. Установка новых офисных приложений, смена хостинг-компании 3. Внедрение аутентификации, проверки контактных данных пользователей	ОПК-3
15.	1	Принципом информационной безопасности является принцип недопущения: 1. Неоправданных ограничений при работе в сети (системе) 2. Рисков безопасности сети, системы 3. Презумпции секретности	ОПК-3
16.	1	Принципом политики информационной безопасности является принцип: 1. Невозможности миновать защитные средства сети (системы) 2. Усиления основного звена сети, системы 3. Полного блокирования доступа при риск-ситуациях	ОПК-3
17.	1	Принципом политики информационной безопасности является принцип: 1. Усиления защищенности самого незащищенного звена сети (системы) 2. Перехода в безопасное состояние работы сети, системы 3. Полного доступа пользователей ко всем ресурсам сети, системы	ОПК-3
18.	1	Принципом политики информационной безопасности является принцип: 1. Разделения доступа (обязанностей, привилегий) клиентам сети (системы) 2. Одноуровневой защиты сети, системы 3. Совместимых, однотипных программно-технических средств сети, системы	ОПК-3
19.	2	К основным типам средств воздействия на компьютерную сеть относится: 1. Компьютерный сбой 2. Логические закладки («мины») 3. Аварийное отключение питания	ОПК-3
20.	3	Когда получен спам по e-mail с приложенным файлом, следует: 1. Прочитать приложение, если оно не содержит ничего ценного – удалить 2. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама 3. Удалить письмо с приложением, не раскрывая (не читая) его	ОПК-3
21.	3	Принцип Кирхгофа: 1. Секретность ключа определена секретностью открытого сообщения 2. Секретность информации определена скоростью передачи данных 3. Секретность закрытого сообщения определяется секретностью ключа	ОПК-3

22.	2	Наиболее распространены угрозы информационной безопасности корпоративной системы: 1. Покупка нелицензионного ПО 2. Ошибки эксплуатации и неумышленного изменения режима работы системы 3. Сознательного внедрения сетевых вирусов	ОПК-3
23.	3	Наиболее распространены угрозы информационной безопасности сети: 1. Распределенный доступ клиент, отказ оборудования 2. Моральный износ сети, инсайдерство 3. Сбой (отказ) оборудования, нелегальное копирование данных	ОПК-3
24.	2	Наиболее распространены средства воздействия на сеть офиса: 1. Слабый трафик, информационный обман, вирусы в интернет 2. Вирусы в сети, логические мины (закладки), информационный перехват 3. Компьютерные сбои, изменение администрирования, топологи	ОПК-3
25.	1	Утечкой информации в системе называется ситуация, характеризуемая: 1. Потерей данных в системе 2. Изменением формы информации 3. Изменением содержания информации	ОПК-3
26.	1	Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются: 1. Целостность 2. Доступность 3. Актуальность	ОПК-3
27.	1	Угроза информационной системе (компьютерной сети) – это: 1. Вероятное событие 2. Детерминированное (всегда определенное) событие 3. Событие, происходящее периодически	ОПК-3
28.	3	Информация, которую следует защищать (по нормативам, правилам сети, системы) называется: 1. Регламентированной 2. Правовой 3. Защищаемой	ОПК-3
29.	1	Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:	ПК-9

		1. Программные, технические, организационные, технологические 2. Серверные, клиентские, спутниковые, наземные 3. Личные, корпоративные, социальные, национальные	
30.	1	Окончательно, ответственность за защищенность данных в компьютерной сети несет: 1. Владелец сети 2. Администратор сети 3. Пользователь сети	ПК-9
31.	1	Политика безопасности в системе (сети) – это комплекс: 1. Руководств, требований обеспечения необходимого уровня безопасности 2. Инструкций, алгоритмов поведения пользователя в сети 3. Нормы информационного права, соблюдаемые в сети	ПК-9
32.	3	Наиболее важным при реализации защитных мер политики безопасности является: 1. Аудит, анализ затрат на проведение защитных мер 2. Аудит, анализ безопасности 3. Аудит, анализ уязвимостей, риск-ситуаций	ПК-9
33.	это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением. Другими словами, это совершение с информацией действий, результатом которых является невозможность получения или использование ее по назначению при полной сохранности самой информации	Блокирование компьютерной информации	ПК-9

34.	как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. В случае использования скомпрометированной информации потребитель подвергается опасности принятия неверных решений со всеми вытекающими последствиями.	Компрометация информации	ПК-9
35.	это протокол управления параллельностью, основная цель которой состоит в установлении глобальной очередности выполнения транзакций, при которой боле старые	Метод использования временных отметок	ПК-9

	транзакции (транзакции с меньшим значением временной отметки) имеют более высокий приоритет при разрешении возникающих конфликтов.		
36.	Существуют некоторые свойства, которыми должна обладать любая из транзакций: • Атомарность – любая транзакция представляет собой неделимую единицу работы, которая может быть либо выполнена вся целиком, либо не выполнена вовсе. • Согласованность – каждая транзакция должна переводить БД из одного согласованного состояния в другое согласованное состояние. • Изолированность – все транзакции выполняются независимо одна от другой. Другими	Свойства транзакций	ПК-9

	словами, промежуточные результаты незавершенной транзакции не должны быть доступны тругим транзакциям • Продолжительность – результаты успешно завершенной транзакции должны сохраняться в базе данных постоянно и не должны быть утеряны в результате последующих сбоев		
37.	прикладными программами. Он взаимодействует с планировщиком, отвечающим за реализацию выбранной стратегии управления параллельностью. В некоторых случаях планировщик называют менеджером блокировки, если используемых протокол управления параллельностью строится на основе блокировки. Цель	Менеджер транзакций	ПК-9

	работы планировщика состоит в достижении максимально возможного уровня параллельности, при условии исключения влияния параллельно выполняющихся транзакций друг на друга, поскольку это может послужить источником нарушения согласованности базы данных.		
38.	это управление физической реализацией приложений баз данных: физическое проектирование базы данных и ее реализация, организация поддержки целостности и защиты данных, наблюдение за текущим уровнем производительности системы, а также реорганизация базы данных по мере необходимости.	Администрирование базы данных	ПК-9
39.	• Оценка и выбор целевой СУБД	Задачи администрирования БД	ПК-9

	• Физическое проектирование БД • Реализация физического проекта БД в среде целевой СУБД • Определение требований защиты и поддержки целостности данных • Взаимодействие с разработчиками приложений БД • Разработка стратегии тестирования • Обучение пользователей • Ответственность за сдачу в эксплуатацию готового приложения БД • Контроль текущей производительности системы и соответствующая настройка БД • Регулярное резервное копирование • Разработка требуемых механизмов и процедур восстановления • Обеспечение полноты используемой документации, включая		

	материалы, разработанные внутри организации • Поддержка актуальности используемого программного продукта и аппаратного обеспечения, включая заказ и установку пакетов обновления в случае необходимости.		
40.	Этот метод предусматривает организацию на время выполнения транзакции двух таблиц страниц – текущую и теневую. Когда транзакция начинает работать, обе таблицы идентичны. Теневая таблица страниц никогда не изменяется и может быть использована для восстановления БД в случае отказа системы. В ходе выполнения транзакции текущая таблица страниц используется для записи в БД всех вносимых изменений. После	Метод теневых страниц	ПК-9

	завершения транзакции текущая таблица страниц становится теневой таблицей. Этот метод имеет ряд преимуществ перед предыдущими методами: - исключается нагрузка, связанная с ведением журнала транзакций; - процесс восстановления происходит значительно быстрее, поскольку нет необходимости в повторном прогоне или откате операций. Однако ему свойственны и определенные недостатки: фрагментация данных и необходимость периодического выполнения процедуры сборки мусора для возвращения в систему неиспользуемых блоков памяти.		
41.	При использовании этого протокола все изменения вносятся в	Метод восстановления с использованием немедленного обновления	ПК-9

	БД сразу же после из выполнения в транзакции, не дожидаясь ее завершения. Помимо необходимости повторного прогона изменений, выполненных транзакциями, закончившимися до появления сбоя, в данном случае может потребоваться выполнить откат изменений, внесенных транзакциями, которые не были завершены к этому моменту.		
42.	При использовании этого протокола обновления не заносятся в БД до тех пор, пока транзакция не выдаст команду фиксации выполненных изменений. Если выполнение транзакции будет прекращено до достижения этой точки, никаких изменений в БД выполнено не будет, поэтому не потребуется	Метод восстановления с использованием отложенного обновления	ПК-9

	и их отмена. Однако в данном случае может потребоваться повторный прогон уже завершившихся транзакций, поскольку их результаты могли еще не достичь вторичной памяти.		
43.	Для обеспечения повышенного уровня параллельности может использоваться модернизированный базовый протокол упорядочивания по временным отметкам, который позволяет достичь менее жесткой упорядоченности за счет отмены устаревших операций записи. Это расширение известно, как правило записи Томаса	Правило записи Томаса	ПК-9
44.	периодически выполняемая процедура получения копий базы данных и её файла журнала на носителе, сохраняемой отдельно от системы. Любая СУБД должна предоставлять средства резервного	Резервное копирование и восстановление	ПК-9

	копирования, позволяющие восстанавливать базу в случае её разрушения. Кроме того, рекомендуется создавать резервные копии базы данных и её файла журнала с некоторой установленной периодичностью, а также организовать хранение созданных копий в местах, обеспеченных необходимой защитой. В случае отказа в работоспособности базы данных, резервная копия и зафиксированная в файле журнала определённая информация используется для восстановления базы данных до последнего согласованного состояния. Ведение журнала – процедура создания и обслуживания файла журнала, содержащего сведения обо всех изменениях, внесённых в БД с момента создания последней резервной		

	копии, и предназначенного для обеспечения эффективного восстановления системы в случае её отказа.		
45.	Избирательное управление доступом поддерживается многими СУБД. Избирательное управление доступом поддерживается в языке SQL.В общем случае система безопасности таких СУБД базируется на трех компонентах. Пользователи. СУБД выполняет любое действия с БД от имени какогото пользователя. Каждому пользователю присваивается идентификатор – короткое имя, однозначно определяющее пользователя в СУБД. Для подтверждения того, что пользователь может работать с введенным идентификатором используется пароль.	Избирательное управление доступом	ПК-9

	Таким образом, с помощью идентификатора и пароля производится идентификация и аутентификация пользователя. Объекты БД. По стандарту SQL2 защищаемыми объектами в БД являются таблицы, представления, домены и определенные пользователем наборы символов. Большинство коммерческих СУБД расширяет список объектов, добавляя в него хранимые процедуры и др. объекты. Привилегии. Привилегии показывают набор действий, которые возможно производить над тем или иным объектом. Например, пользователь имеет привилегию для просмотра таблицы.		
46.	Методы обязательного управления доступом применяются к базам	Обязательное управление доступом	ПК-9

	данных, в которых данные имеют достаточно статичную или жесткую структуру, свойственную, например, правительственным или военным организациям. Как уже отмечалось, основная идея заключается в том, что каждый объект данных имеет некоторый уровень классификации, например: секретно, совершенно секретно, для служебного пользования и т.д., а каждый пользователь имеет уровень допуска с такими же градациями, что и в уровне классификации. Тогда на основе этих сведений можно сформулировать два очень простых правила безопасности: а) пользователь имеет доступ к объекту, только если его уровень допуска больше или равен уровню классификации объекта.		

	b) пользователь может модифицировать объект, только если его уровень допуска равен уровню классификации объекта.		
47.	В действующем стандарте языка SQL предусматривается поддержка только избирательного управления доступом. Она основана на двух более или менее независимых частях SQL. Одна из них называется механизмом представлений, который (как говорилось выше) может быть использован для скрытия очень важных данных от несанкционированных пользователей. Другая называется подсистемой полномочий и наделяет одних пользователей пользователям, а также отбирать такие полномочия в случае необходимости.	Поддержка мер обеспечения безопасности в языке SQL	ПК-9

	Механизм представлений языка SQL позволяет различными способами разделить базу данных на части таким образом, чтобы некоторая информация была скрыта от пользователей, которые не имеют прав для доступа к ней. Однако этот режим задается не с помощью параметров операций, на основе которых санкционированные пользователи выполняют те или иные действия с заданной частью данных. Эта функция выполняется с помощью директивы GRANT.		
48.	• Предотвращение – доступ к информации и технологии только для персонала, который имеет допуск от собственника информации. • Обнаружение – обеспечивается раннее	Уровни защиты информации	ПК-9

	обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены. • Ограничение – уменьшается размер потерь, если преступление все-таки произошло. • Восстановление – обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению		
49.	(англ. deface – уродовать, искажать) – тип хакерской атаки, при которой главная (или другая важная) страница веб-сайта заменяется на другую. Эта страница как правило, вызывающего вида (реклама, предупреждение, угроза…). Зачастую доступ ко всему остальному сайту	Дефейс	ПК-9

	блокируется, или же прежнее содержимое сайта вовсе удаляется. Некоторые взломщики делают deface сайта для получения признания в хакерских кругах, повышения своей известности или для того, чтобы указать администратору сайта на уязвимость		
50.	взлом кредитных и дебетовых карт	Кардинг	ПК-9
51.	Взлом программного обеспечения (англ. software cracking) — действия, направленные на устранение защиты программного обеспечения (ПО), встроенной разработчиками для ограничения функциональных возможностей. Последнее необходимо для стимуляции покупки такого проприетарного ПО, после которой ограничения снимаются	Крекинг	ПК-10

52.	или «d.o.s.»-атаки (Denial of Service) – действия, вызывающие «отказ в обслуживании» (d.o.s.) удаленным компьютером, подключенным к сети, говоря на «компьютерном» языке, «зависание» ПК. Одним из методов взлома Интернет-сайтов является «d.o.s.»-атака с последующим запуском программного кода на удаленном сетевом компьютере с правами администратора.	Нюкинг	ПК-10
53.	Как правило, в многопользовательской системе с базой данных одновременно работает несколько пользователей. Некоторые из них могут пытаться одновременно изменять состояние БД. Если они будут делать это независимо, то результирующее состояние БД может оказаться несогласованным.	Неуправляемый параллелизм	ПК-10

54.	называют качественное описание комплекса организационно-технологических и программно-технических мер по обеспечению защиты данных в КС, включает в себя анализ возможных угроз и выбор соответствующих мер противодействия. Политика безопасности, являясь активным компонентом защиты, отображает тот набор законов, правил и норм поведения, которым пользуется конкретная организация при обработке, защите и распространении информации. Выбор конкретных механизмов обеспечения безопасности системы производится в соответствии со сформулированной политикой безопасности.	Политикой безопасности	ПК-10

55.	пассивный компонент системы, хранящий, принимающий или передающий информацию, доступ к которой регламентируется правилами разграничения доступа. Объектами доступа в БД является практически все, что содержит конечную информацию: таблицы (базовые или виртуальные), представления, а также более мелкие элементы данных: столбцы и строки таблиц и даже отдельные поля.	Объект доступа	ПК-10
56.	совокупность правил, регламентирующих права субъектов доступа к объектам доступа. Доступ к информации разделяют на санкционированный и несанкционированный: санкционированный доступ (authorized access to information) - доступ к информации, который	Правила разграничения доступа	ПК-10

	не нарушает установленных правил разграничения доступа, а несанкционированный доступ (unauthorized access to information) - доступ к информации, который нарушает установленные правила разграничения. Контроль доступа обязательно включает идентификацию (персонализацию) и аутентификацию всех субъектов и их процессов и разграничение полномочий субъектов по отношению к объектам с последующей обязательной проверкой введенных полномочий.		
57.	присвоение объектам и субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. Идентификатор доступа	Идентификация	ПК-10

	(access identifier) - уникальный признак объекта или субъекта доступа.		
58.	проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. Тем самым, задача идентификации – ответить на вопрос «кто это?», а задача аутентификации – «а он ли это на самом деле». После идентификации и проверки подлинности устанавливается сфера действий субъекта (доступные ему ресурсы КС). Эту процедуру называют предоставлением полномочий (авторизацией)	Аутентификация	ПК-10
59.	это предоставление прав (или привилегий), позволяющих их владельцу иметь законный доступ к системе или ее	Авторизация	ПК-10

	объектам. Иногда в процесс авторизации включает и идентификацию, и аутентификацию субъектов, требующих получения доступа к объектам. Привилегия доступа (уровень полномочий субъекта доступа) (subject privilege) - совокупность прав доступа субъекта доступа.		
60.	свойство данных сохранять точность и непротиворечивость независимо от внесенных изменений. Зависит от способности информационной системы обеспечить неизменность данных (данные, хранящиеся в системе, не отличаются в семантическом отношении от данных в исходных документах) в условиях случайного и (или) преднамеренного искажения (разрушения). Если быть более точным, то	Целостность данных	ПК-10

	субъектов интересует обеспечение более широкого свойства – достоверности данных (информации), которая складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности данных, т. е. ее не искаженности.		
61.	возможность реализации беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия. Обеспечивается способностью системы обеспечивать своевременный беспрепятственный доступ субъектов к запрашиваемым данным.	Доступность данных	ПК-10
62.	В стандарте SQL определены два оператора GRANT и REVOKE для предоставления и	Операторы SQL предоставления и отмены привилегий	ПК-10

	отмены привилегий соответственно. Оператор предоставления привилегий имеет следующий формат: GRANT {|ALL PRIVILEGES} ON TO {|PUBLIC} [WITH GRANT OPTION] где определяет набор действий из доступного списка действий над объектом данного типа (параметр ALL PRIVILEGES указывает, что разрешены все действия, допустимые для объектов данного типа), определяет имя объекта защиты: таблицы, представления, хранимой процедуры или триггера, определяет список идентификаторов пользователей, кому предоставляются данные привилегии. Вместо списка идентификаторов		

	можно воспользоваться параметром PUBLIC. Параметр WITH GRANT OPTION является необязательным и определяет режим, при котором передаются не только права на указанные действия, но и право передавать эти права другим пользователям. Передавать права в этом случае пользователь может только в рамках разрешенных ему действий. В общем случае набор привилегий зависит от реализации СУБД (определяется производителем).		
63.	Модель целостности Кларка-Вильсона была предложена в 1987 г. как результат анализа практики бумажного документооборота в коммерческих компаниях, эффективной с точки зрения обеспечения	Модель Кларка-Вильсона	ПК-10

	целостности информации. Модель Кларка-Вильсона является описательной и не содержит каких бы то ни было строгих математических конструкций – скорее её целесообразно рассматривать как совокупность практических рекомендаций по построению системы обеспечения целостности в КС. Основные понятия данной модели – это корректность транзакций и разграничение функциональных обязанностей. Модель задает правила функционирования КС и определяет две категории данных и два класса операций над ними. Все содержавшиеся в системе данные подразделяются на контролируемые и на		

	неконтролируемые элементы данных. Целостность первых поддерживается, а целостность вторых никак не контролируется.		