

Автономная некоммерческая организация профессионального образования
«ПЕРМСКИЙ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ» (АНО ПО «ПГТК»)

УТВЕРЖДАЮ
Заместитель директора
по учебно-методической работе

«01» марта 2019 г. О.В. Бушуева

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ПО МЕЖДИСЦИПЛИНАРНОМУ КУРСУ
МДК 02.05. Безопасность информационных систем
для специальности
09.02.03 Программирование в компьютерных системах
(код и наименование специальности)

Квалификация выпускника Техник-программист (базовая подготовка)

Форма обучения

Очная

Пермь, 2019 г

Фонд оценочных средств «МДК 02.05. Безопасность информационных систем» составлен в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.03 Программирование в компьютерных системах (утвержден приказом Министерства образования и науки Российской Федерации от 28.07.2014 г., № 804).

Предназначен для студентов и преподавателей АНО ПО «ПГТК». Автор – составитель: Тимохова Н.А., старший преподаватель.

Фонд оценочных средств учебной дисциплины рассмотрен и одобрен на заседании кафедры математических и естественно-научных дисциплин, протокол, № 06 от «21» января 2019 г.

Рекомендован к утверждению педагогическим советом АНО ПО «ПГТК» (протокол от «05» февраля 2019г. №3)

Оглавление

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ 4
2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ 6

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Область применения фонда оценочных средств (ФОС)

ФОС по дисциплине МДК 02.05. Безопасность информационных систем является частью программы подготовки специалистов среднего звена по специальности 09.02.03 Программирование в

компьютерных системах

Место дисциплины в структуре ППССЗ: ПМ.02 Разработка и администрирование баз данных

Цели и задачи дисциплины – требования к результатам освоения дисциплины

Умения:

- создавать объекты баз данных в современных СУБД и управлять доступом к этим объектам;
- работать с современными case-средствами проектирования баз данных;
- формировать и настраивать схему базы данных;
- разрабатывать прикладные программы с использованием языка SQL;
- создавать хранимые процедуры и триггеры на базах данных;
- применять стандартные методы для защиты объектов базы данных;

Знания:

- основные принципы построения концептуальной, логической и физической модели данных;
- современные инструментальные средства разработки схемы базы данных;
- методы описания схем баз данных в современных СУБД;
- структуры данных СУБД, общий подход к организации представлений, тлищ, индексов и кластеров;
- методы организации целостности данных;
- способы контроля доступа к данным и управления привилегиями;
- основные методы и средства защиты данных в базах данных;
- модели и структуры информационных систем;
- основные типы сетевых топологий, приемы работы в компьютерных сетях;
- информационные ресурсы компьютерных сетей;
- технологии передачи и обмена данными в компьютерных сетях;
- основы разработки приложений баз данных.

Результаты освоения

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 2.1 Разрабатывать объекты базы данных.

ПК 2.2 Реализовывать базу данных в конкретной системе управления базами данных (далее - СУБД). ПК 2.3 Решать вопросы администрирования базы данных.

ПК 2.4 Реализовывать методы и технологии защиты информации в базах данных.

2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Вид промежуточной аттестации: Экзамен

Метод и форма контроля: Тестирование (Опрос) Вид контроля: Ответьте на 24 вопроса теста

Сущность и понятие информационной безопасности, характеристику ее составляющих
Задание №1

Вопрос 1. Выберите правильное определение термина «информационная безопасность» - это

1. защищенность информации и от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести субъектам информационных отношений
2. актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.
3. совокупность сбалансированных интересов личности, общества и государства в различных сферах жизнедеятельности: экономической, внутривнутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других

Вопрос 2. Выберите правильное определение термина «защита информации»

1. комплекс мероприятий, направленных на обеспечение информационной безопасности.
2. спектр интересов субъектов, связанных с использованием информационных систем, которые можно разделить на категории
3. возможность за приемлемое время получить требуемую информационную услугу
4. спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов

Вопрос 3. Соотнесите определения и термины категорий

Целостность	возможность за приемлемое время получить требуемую
информационную	
услугу	

Конфиденциальность	актуальность и непротиворечивость информации,
	ее защищенность от разрушения и
	несанкционированного изменения

Доступность	защита от несанкционированного доступа к информации
-------------	---

Вопрос 4. О каком базовом структурном элементе информационной безопасности идет речь:

достигается предоставлением к ней доступа с наименьшими привилегиями исходя из принципа минимальной необходимой осведомленности (англ. least privilege).

Иными словами, авторизованное лицо должно иметь доступ только к той информации, которая ему необходима для исполнения своих должностных обязанностей.

Конфиденциальность Целостность Доступность

Вопрос 5. О каком базовом структурном элементе информационной безопасности идет речь:

Четкое осуществление операций или принятие верных решений в организации возможно лишь на основе достоверных данных, хранящихся в файлах, базах данных или системах, либо транслируемых по компьютерным сетям. Иными словами, информация должна быть защищена от намеренного, несанкционированного или случайного изменения по сравнению с исходным состоянием, а также от каких-либо искажений в процессе хранения, передачи или обработки

Конфиденциальность

Целостность

Доступность

Оценка	Показатели оценки
--------	-------------------

3 Даны правильные ответы на 3 вопроса

4 Даны правильные ответы на 4 вопроса

5 Даны правильные ответы на 5 вопросов

Место информационной безопасности в системе национальной безопасности страны
Задание №1

Вопрос 1. Система национальных интересов России определяется совокупностью основных интересов.

Соотнесите термины и определения основных интересов:

состоят в обеспечении конституционных прав и свобод, личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии;

включают в себя упрочение демократии, достижение и поддержание общественного согласия, повышение созидательной активности населения и духовное возрождение России

личности состоят в защите конституционного строя, суверенитета и территориальной целостности России, в установлении политической, экономической и социальной стабильности, в безусловном исполнении законов и поддержании правопорядка, в развитии международного сотрудничества на основе партнерства

Вопрос 2. Какой принцип деятельности по обеспечению информационной безопасности заключается в обеспечении прав и свобод человека и гражданина при осуществлении противодействия угрозам информационной безопасности,

недопущении противоправных посягательств на его личность, унижения чести и достоинства человека, произвольного вмешательства в его частную жизнь, личную и семейную тайны, ограничения свободы его информационной деятельности, а также в минимизации ущерба этим правам и свободам в случаях, когда их ограничение осуществляется на законных основаниях.

Принцип гуманизма Принцип законности Принцип конкретности

Вопрос 3. Какой принцип деятельности по обеспечению информационной безопасности состоит в обеспечении безопасности применительно к конкретным жизненным обстоятельствам с учетом разнообразных форм проявления объективных законов на основе достоверной информации как о внутренних и внешних угрозах, так и о возможностях противодействия им. Достоверная информация позволяет установить конкретные формы проявления угроз, определить в соответствии с этим цели и действия по обеспечению безопасности, конкретизировать методы противодействия угрозам, а также необходимые для их реализации силы и средства.

Принцип гуманизма Принцип законности Принцип конкретности

Вопрос 4. Какой принцип деятельности по обеспечению информационной безопасности состоит в нахождении и поддержании необходимого баланса между открытостью деятельности по противодействию угрозам информационной безопасности, позволяющей добиться доверия и поддержки общества, и защитой определенной информации, разглашение которой может снизить эффективность противодействия угрозам безопасности.

Принцип гуманизма

Принцип законности и конституционности

Принцип сочетания гласности и профессиональной тайны

Вопрос 5. Какой принцип деятельности по обеспечению информационной безопасности означает осуществление всех свойственных государственным организациям и должностным лицам функций в строгом соответствии с

действующей конституцией, законами и подзаконными актами, согласно установленной в законодательном порядке компетенции. Строгое и неуклонное соблюдение законности и конституционности должно быть неременным требованием, принципом деятельности не только государственных, но и негосударственных органов, учреждений и организаций.

Принцип гуманизма

Принцип законности и конституционности

Принцип сочетания гласности и профессиональной тайны

Оценка	Показатели оценки
3	Даны правильные ответы на 3 вопроса
4	Даны правильные ответы на 4 вопроса
5	Даны правильные ответы на 5 вопросов

Источники угроз информационной безопасности и меры по их предотвращению Задание №1

Вопрос 1. Выберите источники внутренних угроз

Сотрудники Аппаратные средства Организации Вредоносное программное обеспечение

Вопрос 2. Выберите источники внешних угроз

Аппаратные средства Программное обеспечение Стихийные бедствия Вредоносное программное обеспечение Организации

Вопрос 3. По способам воздействия все меры по минимизации угроз подразделяют на:

правовые (законодательные); психологические; административные; физические; аппаратно-программные.

Вопрос 4. Административные меры по предотвращению угроз информационной безопасности включают:

разработку правил обработки информации в компьютерных информационных системах организацию надежного пропускного режима обеспечение конфиденциальности данных регистрацию и анализ событий, происходящих в компьютерных информационных системах

Вопрос 5. Аппаратно-программные средства защиты, которые реализуют самостоятельно или в комплексе с другими средствами следующие способы защиты:

разграничение доступа к ресурсам компьютерных информационных систем контроль целостности данных

обеспечение конфиденциальности данных

распределение реквизитов разграничения доступа (паролей, полномочий и т.п.) организацию скрытого контроля над работой пользователей и персонала

Оценка	Показатели оценки
--------	-------------------

3	Даны правильные ответы на 3 вопроса
---	-------------------------------------

4	Даны правильные ответы на 4 вопроса
---	-------------------------------------

5	Даны правильные ответы на 5 вопросов
---	--------------------------------------

Современные средства и способы обеспечения информационной безопасности Задание №1

Вопрос 1. Выберите примеры которые относятся к методу обеспечения безопасности информации - **ОГРАНИЧЕНИЕ ДОСТУПА**

Физическая преграда

Система охранной сигнализации	Контрольно-пропускная преграда
Установка специальных фильтров	Применение волоконно-оптических кабелей

Вопрос 2. Выберите угрозы который относится к методу обеспечения безопасности информации - **КОНТРОЛЬ ДОСТУПА К АППАРАТУРЕ**

Изменение и разрушение принципиальной схемы компьютерной системы и аппаратуры Подключения постороннего устройства

Изменения алгоритма работы КС путем использования технологических пультов Применение волоконно-оптических кабелей

Размещение технических средств в отдельных помещениях

Вопрос 3. Выберите действия которые относятся к методу обеспечения безопасности информации - **РАЗГРАНИЧЕНИЕ И КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИИ В СИСТЕМЕ**

Организация доступа пользователей к устройствам памяти Размещение технических средств в отдельных помещениях Разделение информации по виду, характеру, назначению

Разработка должностных инструкций по обеспечению режима секретности Изменения алгоритма работы КС путем использования технологических пультов

Вопрос 4. Выберите пример который относится к методу обеспечения безопасности информации - РАЗДЕЛЕНИЕ ПРИВИЛЕГИЙ НА ДОСТУП

Сейф с несколькими ключами Установка специальных фильтров Разделение информации по виду, характеру, назначению

Вопрос 5. Выберите пример который относится к методу обеспечения безопасности информации - ИДЕНТИФИКАЦИЯ И УСТАНОВЛЕНИЕ ПОДЛИННОСТИ ЛИЧНОСТИ

Системы распознавания образа

Присвоение лицу уникального имени или числа – пароля Метод «запрос-ответ»

Символы исходного текста записанные в одном алфавите, заменяются символами другого алфавита Установка специальных экранов

Оценка Показатели оценки

3 Даны правильные ответы на 3 вопроса

4 Даны правильные ответы на 4 вопроса

5 Даны правильные ответы на 5 вопросов

Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи Задание №1

Вопрос 1. Какое правило конфиденциального документооборота означает, что все операции по приему, отправке, обработке, хранению в организации осуществляются в подразделении (отделе, группе) конфиденциального делопроизводства или специально выделенным сотрудником подразделения общего делопроизводства.

Централизация всех стадий, процедур и операций по обработке и хранению конфиденциальных документов

Пооперационный учет всех действий, совершаемых с конфиденциальными документами, учет каждого факта "жизненного цикла" документа Проверка комплектности, целостности документа при любом перемещении

Вопрос 2. Соблюдение какого правила конфиденциального документооборота необходимо для формирования такого массива данных о документах, который в любой момент времени может дать информацию о месте нахождения каждого документа, операциях, совершенных или совершаемых с ним.

Централизация всех стадий, процедур и операций по обработке и хранению конфиденциальных документов

Пооперационный учет всех действий, совершаемых с конфиденциальными документами, учет каждого факта "жизненного цикла" документа Проверка комплектности, целостности документа при любом перемещении

Вопрос 3. Для выполнения этого правила, конфиденциального документооборота, работник подразделения конфиденциального делопроизводства должен при каждом получении или передаче конфиденциального документа пересчитывать количество листов основного документа, количество приложений и количество листов приложений для подтверждения целостности и комплектности конфиденциального документа. При этом в учетной форме и на самом документе отмечается количество листов основного документа и количество приложений и листов приложений. На документе эти сведения проставляются в составе отметки о поступлении (входящем штампе), где наряду с датой и номером поступления указываются перечисленные данные, например:

16.04.2008 вх. № 58к

5 л. + 3 прил. 6 л.

Пооперационный учет всех действий, совершаемых с конфиденциальными документами, учет каждого факта "жизненного цикла" документа Проверка комплектности, целостности документа при любом перемещении Письменная фиксация всех обращений персонала к документу

Вопрос 4. Соблюдение этого правила конфиденциального документооборота требует фиксировать в учетных формах не только те действия,

которые санкционированы и совершаются в соответствии с нормативными актами организации, но и несанкционированные действия, совершаемые

с конфиденциальным документом

Пооперационный учет всех действий, совершаемых с конфиденциальными документами, учет каждого факта "жизненного цикла" документа Проверка комплектности, целостности документа при любом перемещении Письменная фиксация всех обращений персонала к документу

Вопрос 5. Это правило конфиденциального документооборота требует, чтобы в процедуре уничтожения проектов, черновиков, конфиденциальных документов участвовало не менее двух работников. Данная процедура производится только по акту.

Коллегиальность процедуры уничтожения документов, дел и баз данных Проверка комплектности, целостности документа при любом перемещении Письменная фиксация всех обращений персонала к документу

Оценка	Показатели оценки
--------	-------------------

3	Даны правильные ответы на 3 вопроса
---	-------------------------------------

4	Даны правильные ответы на 4 вопроса
---	-------------------------------------

Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности Задание №1

Вопрос 1. Соотнесите категории конфиденциальности защищаемой информации с определениями: Строго конфиденциальная информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства, а также информация, ограничение на распространение которой введены решениями руководства организации

Конфиденциальная информация, ограничения на распространение которой вводятся решением руководства организации в соответствии с предоставленными ему как собственнику информации действующим законодательством правами

Открытая информация, обеспечения

конфиденциальности (введения ограничений на распространение) которой не требуется
Вопрос 2. Соотнесите категории целостности защищаемой информации с определениями:

Высокая к данной категории относят

информацию, несанкционированная модификация или фальсификация которой может привести к нанесению значительного прямого ущерба организации

Низкая данная категория включает

в себя информацию, несанкционированная модификация, подмена или удаление которой может привести к нанесению незначительного косвенного ущерба организации, ее клиентам, партнерам или сотрудникам

Нет требований к данной категории

относится информация, к обеспечению целостности (и аутентичности) которой требований не

предъявляется

Вопрос 3. Соотнесите категории доступности защищаемой информации с определениями:

Беспрепятственная доступность

доступ к задаче должен обеспечиваться в любое время

Высокая доступность доступ к задаче осуществляется без существенных временных задержек
Средняя доступность доступ к задаче может обеспечиваться с существенными временными задержками

Низкая доступность временные задержки при доступе к задаче практически не лимитированы

Оценка Показатели оценки

3 Дан правильный ответ на 1 вопрос

4 Даны правильные ответы на 2 вопроса

5 Даны правильные ответы на 3 вопроса

Классифицировать основные угрозы безопасности информации Задание №1

Вопрос 1. Выберите угрозы, которые относятся к классификации по природе возникновения:

Независимо от активности автоматизированной системы Естественные угрозы
Искусственные угрозы Программно-аппаратные средства

Вопрос 2. Выберите угрозы, которые относятся к классификации по источнику угроз

Природная среда Человек

Программно-аппаратные средства На внешних запоминающих угрозах Угрозы доступа к информации, циркулирующей в линиях связи

Вопрос 3. Выберите угрозы, которые относятся к классификации по положению источника угроз

Вне контролируемой зоны Искусственные угрозы Халатность персонала Непосредственно в автоматизированной системе

Вопрос 4. Выберите угрозы, которые относятся к классификации по степени воздействия на автоматизированную систему

Пассивные угрозы Активные угрозы Халатность персонала Искусственные угрозы

Вопрос 5. Выберите угрозы, которые относятся к классификации по текущему месту расположения информации

На внешних запоминающих устройствах

Угрозы доступа к информации, циркулирующей в линиях связи Человек Природная среда

Оценка Показатели оценки

- 3 Даны правильные ответы на 3 вопроса
- 4 Даны правильные ответы на 4 вопроса
- 5 Даны правильные ответы на 5 вопросов

Применять основные правила и документы сертификации Российской Федерации Задание №1

Вопрос 1. Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации

Указанные средства подлежат обязательной проверке федеральных органов Указанные средства подлежат обязательной проверке службой безопасности

Вопрос 2. Соотнесите основные схемы проведения сертификации средств защиты информации:

для единичных образцов средств защиты информации проведение испытаний этих образцов на соответствие требованиям по защите информации

для серийного производства средств защиты информации проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью

характеристик сертифицированных средств защиты информации, определяющих выполнение этих требований

Вопрос 3. В каких случаях Федеральный орган по сертификации и органы по сертификации средств защиты информации имеют право приостанавливать или аннулировать действие сертификата:

изменение нормативных и методических документов по защите информации в части требований к средствам защиты информации, методам испытаний и контроля;

изменение технологии изготовления, конструкции (состава), комплектности средств защиты информации и системы контроля их качества;

отказ изготовителя обеспечить беспрепятственное выполнение своих полномочий лицами, осуществляющими государственные контроль и надзор, инспекционный контроль за сертификацией и сертифицированными средствами защиты информации.

проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации,

определяющих выполнение этих требований проведение испытаний этих образцов на соответствие требованиям по защите информации

Вопрос 4. Выберите участников сертификации средств защиты информации:

федеральный орган по сертификации;

органы по сертификации средств защиты информации; испытательные лаборатории; изготовители-продавцы, исполнители продукции. конструкторы-испытатели правоохранительные органы

Вопрос 5. Срок действия сертификата средств защиты информации не может превышать:

пяти лет десяти лет трех лет

Оценка	Показатели оценки
--------	-------------------

3	Даны правильные ответы на 3 вопроса
---	-------------------------------------

4	Даны правильные ответы на 4 вопроса
---	-------------------------------------

5	Даны правильные ответы на 5 вопросов
---	--------------------------------------

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п.п.	Содержание изменения	Дата, номер протокола заседания педагогического совета
1	2	3
1	Внесены изменения в перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.	решение от 27.08.2020 №7
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		