Приложение
к ППССЗ по специальности 09.02.07
Информационные системы и программирование

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ УЧЕБНОЙ ПРАКТИКЕ

## УП.12.01 УЧЕБНАЯ ПРАКТИКА
## ПМ.12 РАЗРАБОТКА ДЕЦЕНТРАЛИЗОВАННЫХ ПРИЛОЖЕНИЙ
## 09.02.07 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ПРОГРАММИРОВАНИЕ

базовый уровень подготовки

Год начала подготовки – 2024

2023

# Оглавление

## 1. Паспорт фонда оценочных средств

Фонд оценочных средств предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной практики профессионального модуля ПМ.12. Разработка децентрализованных приложений.

ФОС включают контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме дифференцированного зачёта.

ФОС разработан на основании положений:

программы подготовки специалистов среднего звена по специальности СПО 09.02.07 Информационные системы и программирование;

программы учебного модуля;

учебного плана по специальности СПО 09.02.07 Информационные системы и программирование;

положения «О фонде оценочных средств для проведения текущего контроля успеваемости промежуточной и итоговой аттестации студентов и обучающихся филиала СамГУПС в г. Алатыре».

## 2. Результаты освоения программы учебной практики, подлежащие проверке

### 2.1 Перечень умений, знаний, общих компетенций

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

1.1.1.Перечень общих компетенций

| | |
|---|---|
| ОК 1. | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам; |
| ОК 2. | Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности; |
| ОК 3 | Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях; |
| ОК 4 | Эффективно взаимодействовать и работать в коллективе и команде; |
| ОК 5 | Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста; |
| ОК 6 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения; |
| ОК 7 | Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях; |
| ОК 8 | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности; |
| ОК 9 | Пользоваться профессиональной документацией на государственном и иностранном языках.»; |

1.1.2.Перечень профессиональных компетенций

| | |
|---|---|
| ПК 12.1 | Способность разрабатывать распределенные децентрализованные приложения |
| ПК 12.2 | Способность разрабатывать распределенными приложениями |
| ПК 12.3 | Применять методы хеширования данных, криптографические методы защиты информации и цифровые подписи |

1.1.3. В результате освоения профессионального модуля студент должен:

**иметь практический опыт:**

- работы с системой блокчейн-криптовалют: кошельками, транзакциями, майнингом;
- подготовки к ICO и краудфандингу;
- работы на биржах криптовалют со смарт-контрактами и токенами;
- работы с различными блокчейн-платформами;
- развертывания приватных блокчейн-сетей;
- написания и тестирование смарт-контрактов;
- разработка распределенных децентрализованных приложений на различных блокчейн-платформах.

**уметь:**

- разрабатывать web-сервисы для работы с различными блокчейн-платформами;
- разрабатывать интерфейсы для взаимодействия с распределенными приложениями;

• разрабатывать децентрализованные приложения;
• применять методы хеширования данных, криптографические методы защиты информации и цифровые подписи;
• использовать возможности различных блокчейн-платформ для проведения транзакций;
• разрабатывать скрипты и смарт-контракты, а также их тестировать.

**знать:**

• принципы построения решений «бизнес для бизнеса» (B2B) и «бизнес для потребителя» (B2C);
• принципы применения технологии блокчейн для приложений за рамками финансовых областей;
• принципы работы с криптовалютами, смарт-контрактами и области применения ICO;
• отношение регуляторов к криптоактивам в разных странах мира;
• технологии разработки web-сервисов и интерфейсов для взаимодействия с распределенными приложениями;
• технологии разработки децентрализованных приложений;
• преимущества и недостатки распределенных систем;
• технологии идентификации, аутентификации, авторизации;
• методы хеширования данных, криптографические методы защиты информации и цифровых подписей;
• принципы работы, возможности и ограничения технологии блокчейна;
• возможности блокчейн биткоина;
• принципы работы блокчейн Ethereum;
• принципы разработки блокчейна для консорциума предприятий.

## 3. Типовые задания для оценки освоения программы учебной практики

Работа содержит задания по разработке программного обеспечения с использованием инструментальных средств. Все документы должны быть выполнены максимально точно по представленному образцу.

Результаты выполнения задания оформляются в виде отдельных файлов соответствующих форматов и сохраняются на ПК. Для проверки и оценки результаты выполнения экзаменационного задания предоставляются в электронном виде.

В процессе выполнения задания вы можете воспользоваться методическими пособиями, предоставленной учебной литературой и информацией сети Интернет.

Тестирование:

**Тест №1**

Инструкция: выберите один правильный ответ

1. В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долларов США во Внешэкономбанке)?

1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

2. Сколько выделено основных составляющих национальных интересов Российской Федерации в информационной сфере?

1. 2;
2. 3;
3. 4;
4. 5;
5. 6.

3. Активный перехват информации это перехват, который:

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

4. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:

1. надежная защита личной и имущественной безопасности;
2. обеспечение научно обоснованного и гарантированного государством

минимума материальных и экологических условий;
3. преодоление конфронтации в обществе, достижение национального согласия;
4. обеспечение суверенитета и территориальной целостности России.

5. К правовым методам защиты информации относится:
1. разработка нормативно правовых актов, регламентирующих отношения в информационной сфере;
2. создание и совершенствование системы обеспечения ИБ РФ;
3. разработка, использование и совершенствование средств защиты процессов и программ;
4. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
5. формирование системы мониторинга показателей и характеристик ИБ РФ.

6. В стандарте «Оранжевая книга» фундаментальное требование, которое относится к группе Подотчетность:
1. управляющие доступом метки должны быть связаны с объектами;
2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
3. индивидуальные субъекты должны идентифицироваться;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

7. К источникам защищаемой информации относится:
1. электрические поля;
2. магнитные поля;
3. электромагнитные поля;
4. черновики и отходы производства;
5. элементарные частицы;
6. акустические колебания.

8. Информация, использование которой без согласия субъекта может нанести вред его чести, достоинству, деловой репутации:
1. профессиональная тайна;
2. государственная тайна;
3. персональные данные;
4. коммерческая тайна;
5. служебная тайна.

9. В руководящем документе ФСТЭК системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации уровня

государственной тайны, размещенной на носителях одного уровня конфиденциальности – относятся к группе:

1. 1А;
2. 1Г;
3. 2А;
4. 3А;
5. 3Б.

10. Защита информации от несанкционированного воздействия это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

**ТЕСТ №2**

Инструкция: выберите один правильный ответ

1. Какой процент утраты информации от действий собственных сотрудников? 1. 5;
2. 10;
3. 15;
4. 60;
5. 80.

2. Защита информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращениюутечки информации, несанкционированных и непреднамеренных воздействий на неѐ.

3. Пассивный перехват информации это перехват, который:

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

2. Обеспечение национальной безопасности на государственном уровне определяется следующей целью:

1. надежная защита личной и имущественной безопасности;
2. обеспечение научно обоснованного и гарантированного государством минимума материальных и экологических условий;
3. преодоление конфронтации в обществе, достижение национального согласия;
4. обеспечение социально-политической и экономической стабильности страны;
5. обеспечение признанных международным правом интересов граждан России, проживающих в зарубежных странах.

5. К правовым методам защиты информации относится:

1. создание и совершенствование системы обеспечения ИБ РФ;
2. разработка, использование и совершенствование средств защиты процессов и программ;
3. внесение изменений и дополнений в законодательство РФ, регулирующие отношения в области обеспечения ИБ;
4. разработка программ обеспечения ИБ РФ и определение порядка их финансирования;
5. формирование системы мониторинга показателей и характеристик ИБ РФ.

6. В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Подотчетность:

1. управляющие доступом метки должны быть связаны с объектами;
2. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
3. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений; 4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

7. К источникам защищаемой информации относится:

1. электрические поля;
2. сырье;
3. магнитные поля;
4. электромагнитные поля;
5. элементарные частицы;
6. акустические колебания.

8. Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

9. В руководящем документе ФСТЭК системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации уровня не относящейся к государственной тайне, размещенной на носителях одного уровня конфиденциальности – относятся к группе:

1. 1А;
2. 1Г;
3. 2А;
4. 3А;
5. 3Б.

10. Защита информации от непреднамеренного воздействия это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Критерии оценки тестовых заданий.

| Оценка | Число выполненных заданий |
|---|---|
| 5(отлично) | все |
| 4(хорошо) | выполнено не полностью |
| 3(удовлетворительно) | выполнено частично |
| 2(неудовлетворительно) | не выполнено |

### 3.1 Основные источники:

Электронные издания (электронные ресурсы)

1. Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : учебное пособие / Ю. А. Котов. — Новосибирск : НГТУ, 2017. — 67 с. — ISBN 978-5-7782-3411-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118230

2. Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, [б. г.]. — Часть 1 — 2017. — 64 с. — ISBN 978-5-7641-1053-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111765

## 1. Контрольно-оценочные материалы для итоговой аттестации

### Вопросы для итогового контроля

1. Что такое сбор информации и каково его предназначение?
2. Что понимается под технологией сбора информации?
3. Чем отличаются понятия «информация» и «данные»?
4. Назовите основные требования к сбору данных и к хранимым данным.
5. Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации. Какие еще средства сбора информации вам известны?
6. Какие еще методы сбора данных вам известны?
7. В чем заключается процедура хранения информации?
8. Перечислите основные требования к структурам хранения.
9. Что такое база данных?
10. В чем различие между базой и банком данных?
11. Что такое резервное копирование и для чего оно осуществляется?
12. Что такое архивное копирование и в чем его отличие от резервного копирования?
13. Что такое базовая информационная технология?
14. В чем заключается различие между централизованным и децентрализованным способами обработки информации?
15. Какие режимы обработки информации вам известны?
16. Что такое информационная безопасность?
17. Перечислите важнейшие аспекты информационной безопасности.
18. Перечислите уровни решения проблемы информационной безопасности.
19. Перечислите уровни защиты информации.
20. Охарактеризуйте угрозы информационной безопасности: раскрытия целостности, отказ в обслуживании.
21. Объясните причины компьютерных преступлений.
22. Опишите, как обнаружить компьютерное преступление или уязвимые места в системе информационной безопасности.
23. Опишите основные технологии компьютерных преступлений.
24. Перечислите меры защиты информационной безопасности.
25. Перечислите меры предосторожности при работе с целью защиты информации.
26. Опишите, какими способами можно проверить вводимые данные на корректность.
27. Опишите основные меры защиты носителей информации.
28. Почему подключение к глобальной компьютерной сети Интернет представляет собой угрозу для информационной безопасности?
29. Опишите, как использование электронной почты создает угрозу информационной безопасности. Какие меры обеспечивают безопасное использование e-mail?

**Критерии оценки**

- **оценка «отлично»** выставляется студенту, если дан правильный ответ на

2 теоретических вопроса и выполнены правильно все практические задания;

- - **оценка «хорошо»** если дан правильный ответ на 2 теоретических вопроса и выполнено правильно одно практическое задание или дан правильный ответ на теоретический вопрос и выполнены правильно все практические задания;
- **оценка «удовлетворительно»** если дан правильный ответ на теоретический вопрос и выполнено правильно одно практическое задание или дан правильный ответ на 2 теоретических вопроса, или выполнены правильно 2 практических задания;
- **оценка «неудовлетворительно»** если не дан правильный ответ на 2 теоретических вопроса и не выполнены правильно все практические задания.