Автономная некоммерческая организация высшего образования
"НАЦИОНАЛЬНЫЙ ОТКРЫТЫЙ ИНСТИТУТ Г. САНКТ-ПЕТЕРБУРГ"
Кафедра математических и естественнонаучных дисциплин

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ (ОЗНАКОМИТЕЛЬНОЙ) ПРАКТИКИ

Направление подготовки **09.03.03 Прикладная информатика**

Профиль подготовки: Прикладная информатика в экономике

Квалификация выпускника: бакалавр

Форма обучения – очная, заочная

Санкт-Петербург
2021

Составлены в соответствии с учебным планом и рабочей программой Учебной практики для подготовки бакалавра по направлению подготовки 09.03.03 Прикладная информатика

ОДОБРЕНЫ
на заседании кафедры математических и естественнонаучных дисциплин,
протокол № 1/21 от «_06__»_сентября____2021__г.

Зав. кафедрой _____ к.т.н., проф. Боброва Л.В.
(подпись)

Составитель _____ к.т.н., доцент Боброва Л.В.
(подпись)

Рецензент _____ к.т.н., доцент Лучина Н.А.
(подпись)

Эксперты _____ к.т.н., доцент Сибирев В.Н.
(подпись)

Содержание

1. Цель и задачи дисциплины

Цель дисциплины

получение первичных профессиональных умений в конкретной производственной области, приобретение реального практического опыта навыков самостоятельной работы, необходимых студенту в его дальнейшей профессиональной деятельности, а также закрепление и расширение объема теоретических знаний, полученных в АНО ВО «Национальный открытый институт г. Санкт-Петербург».

Задачами дисциплины является изучение:

Задачи учебной практики

А) осуществить

- ознакомление с нормативными правовыми актами, приказами, должностными инструкциями, регламентирующими деятельность предприятия, принимающего студентов на практику и работу персонала;
- получение навыков работы с документами;
- ознакомление с организационной структурой предприятия, полномочиями руководителей организации, формами их взаимодействия с сотрудниками, структурными подразделениями и иными предприятиями (организациями);
- ознакомление с порядком делопроизводства на предприятии;
- ознакомление с практикой применения информационных технологий в практической хозяйственной деятельности предприятия,

Б) выполнить

- задания, направленные на формирование системных представлений о реальных информационных процессах в подразделениях организации;
- задания, связанные с практической реализацией теоретических положений почерпнутых в процессе изучения базовых и специальных дисциплин;
- задания, направленные на изучение программного обеспечения информационных потоков организации;
- задания, направленные на изучение техническими средствами информационных ресурсов предприятия отраслевой направленности;

В) приобрести навыки

- будущей профессиональной деятельности или в отдельных ее разделах;
- использования методов, применяемых на предприятии для совершенствования организационных структур управления на каждом уровне;
- использования методов, определения эффективности и экономичности структуры управления, механизмы ее совершенствования.

2. Место дисциплины в структуре ООП

Учебная практика является обязательным элементом ООП ВО по направлению подготовки 09.03.03 «Прикладная информатика»**,** входит в состав Блока 2 «Практика» и относится к вариативной части ООП ВО по направлению подготовки 09.03.03 «Прикладная информатика» (Б2.В.01(У).

Предшествующими курсами, на которых непосредственно базируется содержание учебной практики, являются: «Информатика и программирование», «Архитектура электронных вычислительных машин и вычислительные системы», «Операционные системы и среды», «Информационные системы и технологии», «Мировые информационные ресурсы» и др.

3. Организация занятий по Учебной практике

Занятия по Учебной практике представлены следующими видами работы: лекции, практические занятия, самостоятельная работа студентов.

Текущий контроль успеваемости обеспечивает оценивание хода прохождения практики, промежуточная аттестация обучающихся - оценивание промежуточных и окончательных результатов прохождения практики.

Программой практики предусмотрены следующие виды текущего контроля в форме отчетной документации:

- письменный отчет о прохождении практики с оценкой и подписью руководителя практики от предприятия с печатью,
- отзыв о работе с указанием сроков прохождения практики, подписанных руководителем организации и заверенный печатью.

Промежуточная аттестация студентов.

Промежуточная аттестация студентов по Учебной практике проводится в соответствии с Уставом института, локальными актами института и является обязательной.

Зачет принимает лектор с использованием тестовых материалов, либо в устной форме по билетам. При проведении зачета могут быть использованы технические средства.

Знания, умения, навыки студента на зачёте определяются оценками:

«зачтено», «не зачтено» .

Основой для определения оценки служит уровень усвоения студентами материала, предусмотренного рабочей программой.

Критерии оценки по итогам учебной практики:

- оценка «зачтено» - выставляется студенту, если он своевременно в установленные сроки представил на кафедру оформленные в соответствии с требованиями отзыв, отчет о прохождении практики; имеет положительную характеристику от руководителя практики со стороны предприятия; изложил в отчете в полном объеме вопросы по всем разделам практики; во время защиты отчета правильно ответил на все вопросы руководителя практики от филиала.

оценка «незачтено» - выставляется студенту, отсутствующему на закрепленном рабочем месте базы практики или не выполнившему программу практики, или получившему отрицательный отзыв о работе, или ответившему неверно на вопросы руководителя практики от филиала при защите отчета.

4. Паспорт фонда оценочных средств

Процесс прохождения учебной практики направлен на формирование и закрепление следующих компетенций (по ФГОС ВО):

УК-1 – Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

УК-2 – Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;

УК-3 – Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде;

УК-4 – Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах);

УК-5 – Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах;

УК-6 – Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни;

УК-7 – Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;

УК-8 - Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций;

ОПК-1 – Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности;

ОПК-2 – способностью использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности.

В результате прохождения учебной практики студент должен:

Знать:

– технологии и инструментарий поддержки принятий решений с использованием современного программного и технического обеспечения.

Уметь:

- описать характер производственной информационной системы, систему снабжения и сбыта;
- определить степень автоматизации производственных процессов и процессов управления;
- выявить уровень специализации информационных систем предприятия;
- описать производственную структуру предприятия (технологический аспект) и систему организационного устройства (состав отделов и их функции);
- определить характер организационных отношений между структурными подразделениями;
- проводить регламентацию деятельности структурных подразделений, их внутреннюю структуру, связи с другими структурными подразделениями.

Владеть:

- методами, применяемыми на предприятии для совершенствования организационных структур управления на каждом уровне;
- методами определения эффективности и экономичности структуры управления, механизмы ее совершенствования.

Паспорт фонда оценочных средств

Таблица 1

№ п/п	Наименование раздела	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Подготовительный	УК-1, УК-2, УК-3	Тесты
2.	Основной	УК-1, УК-2, УК-3, ОПК-1, ОПК-2	Тесты
3.	Экспериментальный	УК-3, УК-4, УК-5	Тесты
4.	Заключительный	УК-6, УК-7, УК-8, ОПК-1, ОПК-2	Отчет по практике

Таблица 2

Планируемый уровень и результаты обучения для формирования компетенций и критерии их оценивания у студентов, изучающих данную дисциплину

Уровни освоения компетенции	Показатели достижения заданного уровня освоения компетенций	Критерии оценивания результатов обучения			
		2	3	4	5
Базовый уровень	Знать (УК-1, УК-2, УК-3, УК-4, УК-5, УК-6, УК-7, УК-8 ОПК-1, ОПК-2) технологии и инструментарий поддержки принятий решений с использованием современного программного и технического обеспечения	Не знает технологии и инструментарий поддержки принятий решений с использованием современного программного и технического обеспечения	Знает основы технологии и инструментарий поддержки принятий решений с использованием современного программного и технического обеспечения	Знает технологии и инструментарий поддержки принятий решений с использованием современного программного и технического обеспечения	Знает технологии и инструментарий поддержки принятий решений с использованием современного программного и технического обеспечения
	Уметь • (УК-1, УК-2, УК-3, УК-4, УК-5, УК-6, УК-7, УК-8 ОПК-1, ОПК-2) описать характер производственной информационной системы, систему снабжения и сбыта; • определить степень автоматизации производственных процессов и процессов управления; • выявить уровень специализации информационных систем предприятия; • описать производственную структуру предприятия (технологический аспект) и систему организационного устройства (состав отделов и их функции); • определить характер организационных отношений между структурными подразделениями; • проводить	Ошибается в выборе методов и инструментов решения задач	Правильно определяет характер производственной информационной системы, систему снабжения и сбыта	Правильно выбирает степень автоматизации производственных процессов и процессов управления	• Умеет применять уровень специализации информационных систем предприятия; описывать производственную структуру предприятия (технологический аспект) и систему организационного устройства (состав отделов и их функции); определять характер организационных отношений между структурными подразделениями; проводить регламентацию деятельности структурных подразделений, их внутреннюю структуру, связи с другими структурными подразделениями

	регламентацию деятельности структурных подразделений, их внутреннюю структуру, связи с другими структурными подразделениями.				
	Владеть (УК-1, УК-2, УК-3, УК-4, УК-5, УК-6, УК-7, УК-8 ОПК-1, ОПК-2) методами, применяемыми на предприятии для совершенствования организационных структур управления на каждом уровне; методами определения эффективности и экономичности структуры управления, механизмы ее совершенствования.	Не владеет методами, применяемыми на предприятии для совершенствования организационных структур управления на каждом уровне	Владеет некоторыми методами, применяемыми на предприятии для совершенствования организационных структур управления на каждом уровне	Владеет методами, применяемыми на предприятии для совершенствования организационных структур управления на каждом уровне	Владеет методами, применяемыми на предприятии для совершенствования организационных структур управления на каждом уровне; методами определения эффективности и экономичности структуры управления, механизмы ее совершенствования.

5. Фонд оценочных средств

Приложение 1. Типовой вариант теста

1. Информатика - это

A. Наука о всех аспектах переработки информации.
B. Компьютеризация образования.
C. Программа обучения пользованию компьютером.
D. Программа обучения алгоритмическим языкам.
Ответ: A

2. Информационные технологии - это

A. Программное обеспечение информационных систем.
B. Техническое обеспечение информационных систем.
C. Процесс, использующий совокупность средств и методов обработки информации.
D. Методическое обеспечение информационных систем.
Ответ: C

3. Информационный процесс - это

A. Процесс передачи информации.
B. Процесс информатизации общества.
C. Процесс обмена данными.
D. Процесс взаимодействия между двумя объектами материального мира, в результате которого возникает информация.
Ответ : D

4. Что такое информационная система?

A. Пакет программ для переработки информации

B. Взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации.

C. Совокупность технических средств для переработки информации.

D. Набор технических средств и программ.

Ответ: B

5. Информационные ресурсы - это

A. Отдельные документы.

B. Базы данных.

C. Библиотеки.

D. Массивы документов в информационных системах.

Ответ: D

6. Что такое кибернетика?

A. Область человеческой деятельности, связанная с переработкой информации.

B. Наука об общих принципах управления в технике, природе и обществе.

C. Наука о реализации на компьютере различных задач.

D. Наука о системной обеспечении компьютеров.

Ответ: B

7. Концепция внедрения информационных систем управления, которая ориентирована на существующую структуру предприятия, характеризуется :

A. Слабым развитием коммуникаций.

B. Высоким риском от внедрения.

C. Значительными затратами на внедрение.

D. Рационализацией организационной структуры предприятия.

Ответ: A

8. Количество информации, которое содержит сообщение, уменьшающее неопределенность в 2 раза, называется…

A. Байт.

B. Бит

C. Дит.

D. Бод.

Ответ: B

9. Модему, передающему сообщения сос скоростью 28 800 бит/сек для передачи 100страниц текста в 30 строк по 60 символов каждая в кодировке ASCII потребуется … секунд

A. 6,25.

B. 0,02.

C. 6.2,5.

D..50

Ответ: D

10. Укажите последовательность логических операций в порядке убывания их приоритетов :

A, Инверсия, конъюнкция, дизъюнкция, импликация.

B. Инверсия, дизъюнкция, конъюнкция, импликация.

C. Импликация, конъюнкция, дизъюнкция, инверсия.

D. Импликация, дизъюнкция, конъюнкция, инверия.

Ответ: C

11. Первая ЭВМ, в основу которой были положены принципы универсальных ЭВМ, была разработана в

A. Англии (Кембридж) в конце 40-ых годов 20 в.
B. США («Apple») в 1938-м году
C. СССР (УА Наук) в 1940-м году
D. нет правильного ответа

12. ЭВМ классифицируют по

A. все ответы правильные
B. величине (производительности процессора и объёму памяти)
C. по принципу действия
D. по характеру области применения

13. Совокупность бистабильных устройств, предназначенная для хранения информации и быстрого доступа к ней, называется

A. регистром
B. портом
C. периферийным устройством
D. микросхемой

14. Временное переключение микропроцессора на выполнение другой программы с последующим возвратом к прерванной программе называется

A. прерыванием
B. запросом на прерывание
C. сбоем в работе операционной системы
D. нет правильного ответа

15. Прерывания бывают

A. все ответы правильные
B. аппаратные
C. логические
D. программные

16. Система счисления это

A. способ представления чисел с помощью специального алфавита символов
B. способ и методика обработки цифровой информации
C. способ отчётности при выполнении арифметических операций
D. нет правильного ответа

17. Разряд двоичного числа называется

A. бит

B. байт
C. позиция
D. нет правильного ответа

18. Основание системы счисления указывает на

A. количество символов, используемых в этой системе
B. количество допустимых операций в этой системе
C. количество других систем счисления, в которые можно перевести заданное число
D. нет правильного ответа

19. Числовые разряды разбиваются на два поля – мантиссу и порядок

A. в формате с плавающей точкой
B. в формате с фиксированной точкой
C. в двоичной системе счисления
D. нет правильного ответа

20. Понятие «скалярность» подразумевает наличие в архитектуре ЭВМ специального устройства, называемого

A. конвейер
B. контейнер
C. конвертор
D. компилятор

21. Канал (магистраль), связывающий между собой процессор, ОП, кэш-память, контроллеры и разъёмы на материнской плате, называется

A. шиной ПК
B. интерфейсом
C. информационным кабелем
D. нет правильного ответа

22. Электронная схема, реализующая элементарную логическую операцию, называется

A. логическим элементом
B. преобразователем
C. инвертором
D. нет правильного ответа

23. В схемотехнике не существует логический элемент

A. конвейер
B. конъюнктор
C. дизъюнктор
D. инвертор

24. Информация в ЭВМ кодируется

A. в двоичной форме
B. в десятичной форме
C. специальным международным кодом
D. нет правильного ответа

25. Кодированием сигнала называется

A. установление соответствия между уровнями физического и двоичного сигналов
B. преобразование информации из двоичной формы в 16-ричную
C. преобразование информации из 16-ричной формы в двоичную
D. преобразование информации из десятичной формы в двоичную

26. Программная модель микропроцессора состоит из

A. 32-х регистров
B. набора специальных программ
C. набора управляющих программ
D. нет правильного ответа

27. Регистры процессора предназначены для

A. временного хранения информации
B. постоянного хранения информации
C. перекодировки сигналов
D. нет правильного ответа

28. Среди пользовательских регистров микропроцессора 16-тиразрядными являются только

A. сегментные
B. регистры общего назначения
C. регистры состояния и управления
D. нет правильного ответа

29. Физическая память, к которой микропроцессор имеет доступ по шине адреса, называется

A. оперативной памятью
B. кэш-памятью
C. постоянной памятью
D. нет правильного ответа

30. Микропроцессор аппаратно поддерживает две модели использования ОП

A. сегментированную и страничную
B. страничную и секторную

C. виртуальную и сегментированную
D. нет правильного ответа

31. Адрес памяти, выдаваемый на шину адреса микропроцессора, называется

A. физическим
B. сегментным
C. эффективным
D. нет правильного ответа

32. Размер сегмента в ОП равен

A. 64 Кб
B. 64 Мб
C. 64 Кбит
D. нет правильного ответа

33. Разрядность физического адреса памяти в реальном режиме работы микропроцессора равна

A. 20
B. 16
C. 32
D. нет правильного ответа

34. С точки зрения размерности микропроцессор поддерживает следующие типы данных

A. байт, слово, двойное слово
B. байт, слово, тройное слово
C. бит, байт, слово
D. нет правильного ответа

35. Каждая машинная команда состоит из двух частей:

A. операционной и операндной
B. поля метки и поля мнемокода
C. операционной и комментария
D. нет правильного ответа

36. Не может быть выполнена машинная команда, в которой операнды находятся

A. оба в ОП
B. один в ОП, другой в регистре
C. оба в регистрах
D. один в ОП, другой – непосредственно в команде

37. Поле операндов не может содержать

A. 3 элемента
B. 0 элементов
C. 1 элемент
D. 2 элемента

38. В качестве операнда может выступать

A. все ответы правильные
B. значение регистра
C. ячейка ОП
D. значение, непосредственно заданное в команде

39. Создание загрузочного модуля происходит на этапе

A. компоновки программы
B. трансляции программы
C. отладки программы
D. нет правильного ответа

40. Создание объектного модуля происходит на этапе

A. трансляции программы
B. компоновки программы
C. отладки программы
D. нет правильного ответа

41. Файл листинга нужен для

A. локализации синтаксических ошибок
B. представления исходной программы в машинных кодах
C. запуска программы на выполнение
D. локализации логических ошибок

42. Результатом работы компоновщика является файл с расширением

A. exe
B. obj
C. lst
D. crf

43. Укажите неправильный ответ: Отладчик TD

A. позволяет вносить изменения в исходный текст программы
B. не позволяет вносить изменения в исходный текст программы
C. позволяет определить место логической ошибки
D. позволяет определить причину логической ошибки

46. Запуск отладчика для ассемблера производится командной строкой

A. td.exe имя_исполняемого_модуля
B. tlink.exe /v имя_объектного_модуля
C. tasm.exe /zi имя_объектного_модуля
D. нет правильного ответа

47. Организовать циклы позволяют команды

A. нет правильного ответа
B. пересылки данных
C. логические
D. управления состоянием микропроцессора

48. Для взаимодействия с периферийными устройствами используются команды

A. ввода/вывода
B. передачи управления
C. пересылки данных
D. все ответы правильные

49. Для передачи данных служат шины

A. ISA и PCI
B. AMD и AGP
C. EISA и RGB
D. все ответы правильные

50. Для приращения значения счётчика команд в командах цикла предназначена команда

A. inc
B. dec
C. adc
D. нет правильного ответа

51. При выполнении операций сложения двоичных чисел со знаком необходимо анализировать состояние флагов

A. переноса (cf) и переполнения (of)
B. переполнения (of) и знака (sf)
C. переноса (cf) и знака (sf)
D. нет правильного ответа

52. В командах mul и imul использовать непосредственное значение в качестве операнда

A. нельзя
B. можно
C. можно, если оно не превышает 128

D. нет правильного ответа

53. Используя только команды сдвига, нельзя увеличить или уменьшить число

A. в 6 раз
B. в 2 раза
C. в 8 раз
D. в 4 раза

54. Циклический сдвиг влево через флаг выполняет команда

A. rcl
B. rcr
C. rol
D. ror

55. Для преобразования данных по правилам формальной логики служат команды

A. and, or, xor, not
B. shl, shr, sal, sar
C. and, or, inc, not
D. нет правильного ответа

56. Безусловный переход выполняется по команде

A. jmp
B. jcc
C. jcxz
D. нет правильного ответа

57. Прерывание может быть вызвано

A. все ответы правильные
B. нажатием клавиши на клавиатуре
C. поступлением сигналов от внешних устройств
D. нестандартной ситуацией в работе микропроцессора

58. Главное отличие вычислительных систем (ВС) от ЭВМ –

A. в ВС несколько вычислителей, реализующих параллельную обработку данных
B. у ЭВМ выше производительность
C. работа ВС происходит под управлением операционной системы
D. нет правильного ответа

59. Какая аббревиатура не обозначает архитектуру ВС?

A. МКДМ
B. ОКОД

C. ОКМД
D. МКОД

60. В многомашинных системах каждая машина имеет возможность

A. автономной работы под управлением собственной ОС
B. автономной работы под управлением единой ОС
C. доступа к общей ОП
D. нет правильного ответа

61. Логический элемент, реализующий операцию логического умножения, называется

A. конъюнктор
B. дизъюнктор
C. инвертор
D. копмилятор

62. Два или более ПК, объединяемых по топологии «шина» или с помощью коммутатора и являющиеся единым информационно-вычислительным ресурсом называют

A. кластером
B. узлами
C. многоядерным процессором
D. ЛВС

63. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
A. Сотрудники +
B. Хакеры
C. Атакующие
D. Контрагенты (лица, работающие по договору)

64. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
C. Улучшить контроль за безопасностью этой информации +
D. Снизить уровень классификации этой информации

65. Что самое главное должно продумать руководство при классификации данных?
A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
B. Необходимый уровень доступности, целостности и конфиденциальности +
C. Оценить уровень риска и отменить контрмеры
D. Управление доступом, которое должно защищать данные

66. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
A. Владельцы данных

B. Пользователи
C. Администраторы
D. Руководство +

67. Что такое процедура в терминах IT-технологий?

A. Правила использования программного и аппаратного обеспечения в компании
B. Пошаговая инструкция по выполнению задачи +
C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
D. Обязательные действия

68. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

A. Поддержка высшего руководства +
B. Эффективные защитные меры и методы их внедрения
C. Актуальные и адекватные политики и процедуры безопасности
D. Проведение тренингов по безопасности для всех сотрудников

69. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
B. Когда риски не могут быть приняты во внимание по политическим соображениям
C. Когда необходимые защитные меры слишком сложны
D. Когда стоимость контрмер превышает ценность актива и потенциальные потери +

70. Что такое политики безопасности?

A. Пошаговые инструкции по выполнению задач безопасности
B. Общие руководящие требования по достижению определенного уровня безопасности
C. Широкие, высокоуровневые заявления руководства +
D. Детализированные документы по обработке инцидентов безопасности

71. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

A. Анализ рисков
B. Анализ затрат / выгоды +
C. Результаты ALE
D. Выявление уязвимостей и угроз, являющихся причиной риска

72. Что лучше всего описывает цель расчета ALE?

A. Количественно оценить уровень безопасности среды
B. Оценить возможные потери для каждой контрмеры
C. Количественно оценить затраты / выгоды
D. Оценить потенциальные потери от угрозы в год +

73. Что является определением воздействия (exposure) на безопасность?

A. Нечто, приводящее к ущербу от угрозы +
B. Любая потенциальная опасность для информации или систем
C. Любой недостаток или отсутствие информационной безопасности
D. Потенциальные потери от угрозы

74. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов +
B. Контрмер и защитных механизмов
C. Физической безопасности и технических средств защиты

75. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

A. Внедрение управления механизмами безопасности
B. Классификацию данных после внедрения механизмов безопасности

C. Уровень доверия, обеспечиваемый механизмом безопасности +
D. Соотношение затрат / выгод

76. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

A. Только военные имеют настоящую безопасность
B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности +
C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

77. Как рассчитать остаточный риск?

A. Угрозы х Риски х Ценность актива
B. (Угрозы х Ценность актива х Уязвимости) х Риски +
C. SLE х Частоту = ALE
D. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

78. Что из перечисленного не является целью проведения анализа рисков?

A. Делегирование полномочий +
B. Количественная оценка воздействия потенциальных угроз
C. Выявление рисков
D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

79. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

A. Поддержка
B. Выполнение анализа рисков +
C. Определение цели и границ
D. Делегирование полномочий

80. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

A. Чтобы убедиться, что проводится справедливая оценка
B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа +
D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

81. Что является наилучшим описанием количественного анализа рисков?

A. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
B. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
C. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков +
D. Метод, основанный на суждениях и интуиции

82. Почему количественный анализ рисков в чистом виде не достижим?

A. Он достижим и используется
B. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
C. Это связано с точностью количественных элементов
D. Количественные измерения должны применяться к качественным элементам +

83. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

A. Много информации нужно собрать и ввести в программу +
B. Руководство должно одобрить создание группы
C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
D. Множество людей должно одобрить данные

84. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

A. Стандарты
B. Должный процесс (Due process)
C. Должная забота (Due care) +
D. Снижение обязательств

85. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

A. Список стандартов, процедур и политик для разработки программы безопасности
B. Текущая версия ISO 17799
C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
D. Открытый стандарт, определяющий цели контроля +

86. Из каких четырех доменов состоит CobiT?

A. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
B. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка +
C. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
D. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

87. Что представляет собой стандарт ISO/IEC 27799?

A. Стандарт по защите персональных данных о здоровье +
B. Новая версия BS 17799
C. Определения для новой серии ISO 27000
D. Новая версия NIST 800-60

88. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

A. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
B. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень +
C. COSO учитывает корпоративную культуру и разработку политик
D. COSO – это система отказоустойчивости

89. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

A. NIST и OCTAVE являются корпоративными
B. NIST и OCTAVE ориентирован на ИТ +
C. AS/NZS ориентирован на ИТ
D. NIST и AS/NZS являются корпоративными

90. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

A. Анализ связующего дерева
B. AS/NZS
C. NIST
D. Анализ сбоев и дефектов +

91. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

A. Безопасная OECD
B. ISO\IEC
C. OECD +
D. CPTED

92. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

A. гаммирования;
B. подстановки;
C. кодирования;
D. перестановки; +
E. аналитических преобразований.

93. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

A. гаммирования;
B. подстановки;
C. кодирования;
D. перестановки; +
E. аналитических преобразований.

94. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

A. гаммирования; +
B. подстановки;
C. кодирования;
D. перестановки;
E. аналитических преобразований.

95. Защита информации от утечки - это деятельность по предотвращению:

A. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
B. 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;
C. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
D. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; +
E. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

96. Защита информации это:

A. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
B. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

C. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
D. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
E. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё. +

97. Естественные угрозы безопасности информации вызваны:

A. деятельностью человека;
B. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
C. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; +
D. корыстными устремлениями злоумышленников;
E. ошибками при действиях персонала.

98 Искусственные угрозы безопасности информации вызваны:

A. деятельностью человека; +
B. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
C. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
D. корыстными устремлениями злоумышленников;
E. ошибками при действиях персонала.

99 К основным непреднамеренным искусственным угрозам АСОИ относится:

A. физическое разрушение системы путем взрыва, поджога и т.п.;
B. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
C. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
D. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
E. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы. +

100. К посторонним лицам нарушителям информационной безопасности относится:

A. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
B. персонал, обслуживающий технические средства;
C. технический персонал, обслуживающий здание;
D. пользователи;
E. сотрудники службы безопасности.
F. представители конкурирующих организаций. +
G. лица, нарушившие пропускной режим;

101. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

A. черный пиар; +
B. фишинг;
C. нигерийские письма;
D. источник слухов;
E. пустые письма.

102. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

A. черный пиар;

B. фишинг; +
C. нигерийские письма;
D. источник слухов;
E. пустые письма.

103. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

A. детектор; +
B. доктор;
C. сканер;
D. ревизор;
E. сторож.

104. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла

A. детектор;
B. доктор; +
C. сканер;
D. ревизор;
E. сторож.

105. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

A. детектор;
B. доктор;
C. сканер;
D. ревизор; +
E. сторож.

106. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

A. детектор;
B. доктор;
C. сканер;
D. ревизор;
E. сторож. +

107. Активный перехват информации - это перехват, который:

A. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
B. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
C. неправомерно использует технологические отходы информационного процесса;
D. осуществляется путем использования оптической техники;
E. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера. +

108. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

A. активный перехват;
B. пассивный перехват;
C. аудиоперехват; +
D. видеоперехват;
E. просмотр мусора.

109. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

A. активный перехват;
B. пассивный перехват; +
C. аудиоперехват;
D. видеоперехват;
E. просмотр мусора.

110. Перехват, который осуществляется путем использования оптической техники называется:

A. активный перехват;
B. пассивный перехват;
C. аудиоперехват;
D. видеоперехват; +
E. просмотр мусора.

111. К внутренним нарушителям информационной безопасности относится:

A. клиенты;
B. пользователи системы;
C. посетители;
D. любые лица, находящиеся внутри контролируемой территории;
E. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
F. персонал, обслуживающий технические средства.
G. сотрудники отделов разработки и сопровождения ПО;
H. технический персонал, обслуживающий здание +

112. К правовым методам, обеспечивающим информационную безопасность, относятся:

A. Разработка аппаратных средств обеспечения правовых данных
B. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
C. Разработка и конкретизация правовых нормативных актов обеспечения безопасности. +

113. Основными источниками угроз информационной безопасности являются (все указанное в списке):

A. Хищение жестких дисков, подключение к сети, инсайдерство
B. Перехват данных, хищение данных, изменение архитектуры системы +
C. Хищение данных, подкуп системных администраторов, нарушение регламента работы

114. Виды информационной безопасности:

A. Персональная, корпоративная, государственная +
B. Клиентская, серверная, сетевая
C. Локальная, глобальная, смешанная

115. Основными рисками информационной безопасности являются:

A. Искажение, уменьшение объема, перекодировка информации
B. Техническое вмешательство, выведение из строя оборудования сети
C. Потеря, искажение, утечка информации +

116. К основным принципам обеспечения информационной безопасности относится:

A. Экономической эффективности системы безопасности +
B. Многоплатформенной реализации системы
C. Усиления защищенности всех звеньев системы

117. Основными субъектами информационной безопасности являются:

A. руководители, менеджеры, администраторы компаний

B. органы права, государства, бизнеса +
C. сетевые базы данных, фаерволлы

118. К основным функциям системы безопасности можно отнести все перечисленное:

A. Установление регламента, аудит системы, выявление рисков +
B. Установка новых офисных приложений, смена хостинг-компании
C. Внедрение аутентификации, проверки контактных данных пользователей

119. Принципом информационной безопасности является принцип недопущения:

A. Неоправданных ограничений при работе в сети (системе) +
B. Рисков безопасности сети, системы
C. Презумпции секретности

120. Принципом политики информационной безопасности является принцип:

A. Невозможности миновать защитные средства сети (системы) +
B. Усиления основного звена сети, системы
C. Полного блокирования доступа при риск-ситуациях

Приложение 2. Отчет по практике

Главным результатом учебной практики должна быть подготовка и систематизация материала, составляющего содержание отчета по практике.

Отчет является основным документом, характеризующим работу студента во время практики. В отчете должны быть отражены изученные во время практики общие вопросы и основные результаты практической деятельности студента.

Отчет о прохождении учебной практики состоит из следующих элементов:

1. Титульный лист, оглавления, общей части, заключения, списка использованных источников и литературы, отзыва руководителя практики от организации, заверенного печатью организации, а также индивидуального задания руководителя практики от кафедры.
2. Оглавление, составленное в соответствии с программой практики и представленным в отчете материалом.
3. Введение. Во введении формулируется цель и задачи практики.
4. Основная часть отчета.

Основная часть отчета должна состоять из двух разделов. Раздел 1 включает ответы на все вопросы, предусмотренные в программе. Раздел 2 содержит собранные и систематизированные материалы согласно индивидуальному заданию руководителя практики.

Основная часть отчета включает текстовую и фактологическую составляющие. Текстовая часть отчета представляет собой аналитическую записку, касающуюся специфики конкретного предприятия (объекта практики) и не может быть переписана из учебников и учебных пособий.

Фактологическая часть отчета представляется в виде таблиц, графиков, диаграмм и т.д. и логически дополняет текстовую часть отчета.

По каждому разделу отчета необходимо сформулировать выводы.

5. Заключение. В заключении студент формулирует основные проблемы процесса функционирования системы управления организации.
6. Список использованных источников и литературы.
7. Приложения. В приложениях в отчет могут включаться копии документов (нормативных актов, отчетов и др.), изученных и использованных студентом в период прохождения практики, а также таблицы, занимающие более одной страницы; бланки документов, заполненных студентами в процессе сбора материалов; расчеты и другие данные, раскрывающие содержание программы практики.

Требования к оформлению отчета

Текст отчета предоставляется в печатном виде на листах формата А4. Объем отчета должен быть не менее 15 и не более 25 страниц печатного текста. Текст готовится с использованием текстового редактора Microsoft Word (или аналога) через 1,5 интервала с применением 14 размера шрифта Times New Roman.

Все содержащиеся в отчете материалы должны быть помещены в отдельную папку (скоросшиватель) и сброшюрованы.

Приложение 3. Вопросы к зачету

1. Каковы назначение, цели деятельности предприятия (учреждения, организации), в которой проходила практика?
2. Какова структура предприятия (учреждение, организация)?
3. Схема управления предприятием.
4. Анализ вида информации, с которой работает организация (обработка отраслевой информации).
5. Анализ информационных процессов предприятия
6. Анализ информационных ресурсов предприятия .
7. Анализ программного обеспечения предприятия.
8. Анализ технического обеспечения предприятия.
9. Перечислите основные механизмы защиты ПК от несанкционированного доступа.
10. Перечислите основные методы идентификации пользователей.
11. Что такое распознавание в режиме диалога.
12. Что такое распознавание опознавание по специальным идентификационным карточкам.
13. В чем заключается работа хеш-функции
14. Перечислите средства для опознавания компонентов обработки данных.
15. Перечислите задачи защиты информации в сетях ЭВМ.
16. Основное назначение сетевого уровням защиты информации в сети
17. Какой контроль осуществляется на транспортном уровне
18. Что такое криптозащита?
19. Что такое сервис безопасности?
20. Что является гарантом целостности передаваемых данных
21. Перечислите уровни защиты протоколов передачи данных в сети.
22. Назовите особенность защиты информации в вычислительных сетях
23. Назовите место сервисов безопасности в архитектуре информационных систем
24. Что такое служебная тайна?
25. Какие вы знаете грифы ограничения доступа.
26. Перечислите правила доступа к файлам с различным уровнем доступности, если пользователь имеет уровень доступа «Секретно»
27. Что такое симметричное шифрование
28. Перечислите признаки проявления вирусов
29. Перечислите вирусы, классифицируемые по среде обитания
30. Перечислите виды антивирусных программ.
31. Что такое компьютерный вирус, как он проявляется и какие средства используются для защиты от него?
32. Что такое спам.
33. Перечислите методы защиты от спамов.

6. Экспертное заключение на ФОС по Учебной практике

Экспертиза фонда оценочных средств по Учебной практике для подготовки бакалавров по направлению подготовки 09.03.03 Прикладная информатика проводилась с целью установления соответствий: требованиям ФГОС ВО; целям и задачам реализации основной образовательной программы по направлению и профилю подготовки; целям и задачам рабочей программы реализуемой учебной дисциплины.

В фонде оценочных средств Учебной практике представлены оценочные средства сформированности компетенций выпускника УК-1, УК-2, УК-3, УК-4, УК-5, УК-6, УК-7, УК-8 ОПК-1, ОПК-2.

Фонд оценочных средств включает:

а) паспорт фонда оценочных средств по дисциплине;

б) фонд оценочных средств: тестовые задания;

в) фонд промежуточной аттестации.

Проведенная экспертиза позволила сделать заключение о соответствии фонда оценочных средств по Учебной практике для подготовки бакалавров по направлению подготовки:

требованиям ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика;

целям и задачам реализации основной образовательной программы по направлению подготовки 09.03.03 Прикладная информатика;

целям и задачам рабочей программы Учебная практика по формированию следующих результатов обучения:

Знания:

– технологии и инструментарий поддержки принятий решений с использованием современного программного и технического обеспечения.

Умения:

- описать характер производственной информационной системы, систему снабжения и сбыта;
- определить степень автоматизации производственных процессов и процессов управления;
- выявить уровень специализации информационных систем предприятия;
- описать производственную структуру предприятия (технологический аспект) и систему организационного устройства (состав отделов и их функции);
- определить характер организационных отношений между структурными подразделениями;
- проводить регламентацию деятельности структурных подразделений, их внутреннюю структуру, связи с другими структурными подразделениями.

Навыки:

- методами, применяемыми на предприятии для совершенствования организационных структур управления на каждом уровне;
- методами определения эффективности и экономичности структуры управления, механизмы ее совершенствования.

Фонд оценочных средств отвечает основным принципам и подготовлен в соответствии с требованиями Положения о фонде оценочных средств

Представленный ФОС по Учебной практике рекомендуется утвердить в качестве ФОС по Учебной практике

Сибирев В.Н., к.т.н., профессор кафедры математических и естественнонаучных дисциплин

Лучина Н.А., к.т.н., доцент, Зам. Генерального директора ООО «Ленстройматериалы»

7. Лист регистрации изменений

Номер изменения	Дата	Страницы с изменениями	Перечень и содержание откорректированных разделов рабочей программы