Федеральное агентство по рыболовству
БГАРФ ФГБОУ ВО «КГТУ»
Калининградский морской рыбопромышленный колледж

Утверждаю
Заместитель начальника колледжа
по учебно-методической работе

Подписано цифровой подписью: Колесниченко Андрей Игоревич
Причина: Я утвердил этот документ
Дата: 14 Март 2025 г. 11:09:54
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН ЮЛ=7710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=г. Москва, C=RU, O=Казначейство России, CN=Федеральное казначейство

А.И.Колесниченко

ПМд.07 ЦИФРОВИЗАЦИЯ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Методическое пособие для выполнения самостоятельных работ
по специальности

38.02.01 Экономика и бухгалтерский учет (по отраслям)

МО–38 02 01-ПМд.07.СР

РАЗРАБОТЧИК	Богуш Е.О
ЗАВЕДУЮЩИЙ ОТДЕЛЕНИЕМ	Цепеляева Н.Ф.
ГОД РАЗРАБОТКИ	2023
ГОД ОБНОВЛЕНИЯ	2025

СОДЕРЖАНИЕ

Введение

Методические рекомендации по выполнению самостоятельной внеаудиторной работы составлены в соответствии с рабочей программой ПМд.07 Цифровизация экономической деятельности по специальности 38.02.01 «Экономика и бухгалтерский учет (по отраслям)»

Самостоятельная работа – это деятельность обучающихся в процессе обучения и во внеаудиторное время, выполняемая по заданию преподавателя, но без его непосредственного участия.

На самостоятельную внеаудиторную работу по ПМд.07 Цифровизация экономической деятельности по специальности отведено 4 академических пятом семестре.

Цель внеаудиторной самостоятельной работы:

- закрепить знания и умения по темам и разделам курса;
- расширить знания по отдельным темам;
- сформировать умения самостоятельного изучения элементов курса, пользоваться дополнительной учебной литературой, интернетом;
- развитие самостоятельности, организованности, ответственности;
- работать над формированием общих и профессиональных компетенций, необходимых для осуществления профессиональной деятельности.

Внеаудиторная самостоятельная работа выполняется в отдельных тетрадях в виде конспекта (реферата, презентации).

Критериями оценки результатов самостоятельной работы являются:

- уровень усвоения учебного материала;
- обоснованность и чёткость изложения ответа;
- оформление материала в соответствии с требованиями.

Итоговая оценка выставляется с учётом результатов выполнения самостоятельной внеаудиторной работы.

В результате выполнения самостоятельной работы в процессе изучения ПМд.07 Цифровизация экономической деятельности по специальности обучающийся должен:

В результате освоения учебной дисциплины обучающийся должен

уметь:

- пользоваться автоматизированными системами
- применять специализированное программное обеспечение для сбора, хранения и обработки бухгалтерской информации

В результате освоения учебной дисциплины обучающийся должен

знать:

- назначение, принципы организации и эксплуатации бухгалтерских информационных
- основные понятия автоматизированной обработки информации

- Знаначение, состав, основные характеристики компьютерной и организационной техники

Рабочая программа направлена на формирование у обучающихся следующих компетенций:

ПК 7.1. Применять инфокоммуникационные технологии в бухгалтерском учете.

ПЕРЕЧЕНЬ САМОСТОЯТЕЛЬНЫХ РАБОТ

№ работы	Тема самостоятельной работы	Количество часов
Раздел 2. Основы цифровой экономики		
Тема 2.3 Организационные основы и цифровая безопасность		
1	Восстановление файлов. Ограничение доступа к информации	2
Раздел 3. Трансформация бизнеса в цифровой экономике		
Тема 3.3 Применения блокчейна в бухгалтерском учете		
2	*Тенденции и перспективы развития систем обработки экономической информации*	2
Итого:		**4**

Раздел 2. Основы цифровой экономики

Тема 2.3 Организационные основы и цифровая безопасность

Самостоятельная работа №1. Восстановление файлов. Ограничение доступа к информации

Цель работы:

1. Изучить восстановление файлов и организацию ограничений доступа к информации.

2. Знать как можно восстановить стертую информацию и как организовать ограничения доступа к информации.

Формируемые общие и профессиональные компетенции: ПК 7.1

Литература: [1,2,3,4,5,6], конспект

Порядок выполнения работы:

I. Восстановление файлов.

Существует несколько способов восстановления файлов, ошибочно удаленных с диска, а также поврежденных вследствие появления логических ошибок в файловой структуре и возникновения физических дефектов на магнитном диске. Для этих целей применяются утилиты MS-DOS, утилиты пакета Norton Utilities и служебные программы Windows 95.

*Под **восстановлением файлов** понимается воссоздание их первоначального содержания в исходной форме.*

Частным случаем восстановления файлов является извлечение файлов из резервных копий, полученных при помощи программ резервного копирования и архивирования, и «лечение» файлов, пораженных программным вирусом. Удаление файлов производится при форматировании диска и при использовании соответствующих команд операционных-систем и оболочек.

Восстановление файлов на отформатированном диске возможно, если было выполнено *безопасное* или *быстрое* форматирование с сохранением образа системной области диска, содержащей загрузочную запись, таблицу размещения файлов (FAT) и корневой каталог. Восстановление файлов после такого форматирования основано на том, что при форматировании стираются данные только из системной области диска, так что доступ к файлам становится невозможным, хотя содержимое файлов сохраняется. Системную область можно сохранить при помощи утилиты Imageиз комплекта Norton Utilities или при помощи утилиты Mirrorкомплекта PCTools фирмы Central Point Software. Можно восстанавливать как гибкие, так и жесткие диски. Полное восстановление диска

возможно только в том случае, если после его форматирования не была записана новая информация; иначе возможно лишь частичное восстановление. Восстановление информации на диске после ошибочного форматирования можно выполнить при помощи команды UNFORMAT или утилиты UnFormat. входящей в комплект утилит Norton Utilities.

Утилита UnFormat комплекта утилит Norton Utilities может быть использована только в среде MS-DOS. Утилита функционирует в диалоговом режиме. Она может быть использована также для восстановления системной области диска, поврежденной вследствие сбоя питания или действий компьютерных вирусов.

Утилита Image сохраняет образ диска в файле IMAGE.DAT в корневом каталоге и создает скрытый индексный файл IMAGE.IDX. В MS-DOS утилита Image функционирует только в командном режиме. В Windows используется утилита Image32, функционирующая в диалоговом режиме. Запуск ее осуществляется при помощи Проводника или из командной строки меню Пуск. Рекомендуется помещать команду IMAGE [диск:] в файл AUTOEXEC.BAT (MS-DOS) или в папку Автозагрузка (Windows).

Восстановление файлов, удаленных командами операционных систем или программных оболочек, основано на том, что при удалении файлов удаляет только первую букву имени файла, заменяя ее соответствующим кодом, указывающим, что данный элемент свободен для размещения других файлов.

Восстановление файлов можно выполнить при помощи:

- команд MS-DOS UNDELETE и MWUNDEL;
- утилит UnErase и UnErase Wizard комплектаNorton Utilities.

Команды UNDELETE и MWUNDELпозволяют не только восстанавливать удаленные файлы, но и *защищать* файлы от удаления. Обе утилиты выполняют одинаковые функции по защите и восстановлению файлов, а различие состоит в том, что утилита UNDELETEзапускается из командной строки, а MWUNDEL - в окне Windowsи имеет удобный диалоговый интерфейс.

Хотя функция защиты файлов от удаления не является главной для команд UNDELETEи MWUNDEL, тем не менее, она определяет возможные методы восстановления удаленных файлов, которые основаны на использовании *трехуровней защиты.* В документации по MS-DOS эти уровни имеют названия:

DeleteSentry, DeleteTrackerи Standard. Для обеспечения восстановления файлов с использованием первых двух уровней защиты необходимо *до удаления файлов* запустить команду UNDELETEили MWUNDEL в режиме защиты, после чего она остается резидентной в ОЗУ.

Уровень DeleteSentry является наивысшим. Он предоставляет наибольшие гарантии восстановления удаленных файлов. При его использовании утилиты UNDELETEи MWUNDELсоздают скрытый каталог с именем SENTRY. По команде удаления файла программа UNDELETE (MWUNDEL), хранящаяся в ОЗУ резидентно, перемещает удаляемый файл в каталог SENTRY без изменения записи о размещении файла в таблице размещения файлов (FAT). Во время восстановления файла по команде UNDELETE (MWUNDEL) MS – DOS возвращает файл в каталог, в котором он находился до удаления.

Суммарный размер файлов, хранящихся в каталоге SENTRY, ограничивается величиной, равной примерно 7% от общего объема диска. Если при удалении файлов эта величина будет превышена, то UNDELETE (MWUNDEL) удалит из каталога SENTRY наиболее старые файлы, чтобы освободить место для размещения новых.

Уровень DeleteTracker обеспечивает уровень защиты, средний между DeleteSentry и Standard. Он использует скрытый файл PCTRACK.DEL, в который записывается информация о размещении удаляемых файлов. По команде удаления файла MS – DOS изменяет FAT таким образом, что место, занимаемое удаленным файлом, может быть использовано для размещения другого файла. Следовательно, сто процентное восстановление удаленного файла на этом уровне возможно, если на диск после удаления файла не был помещен другой файл. Файл PCTRACK.DEL занимает на диске значительно меньше места, чем файлы каталога SENTRY.

Уровень защиты Standard является низшим уровнем. Он доступен во все время работы компьютера и обеспечивает наименьшую степень защиты от ошибочного удаления файлов. В то же время он не требует использования резидентно загруженной программы UNDELETE (MWUNDEL) при удалении файлов и места на жестком диске. На этом уровне не гарантируется полное восстановление файлов, если после их удаления на диск был записан новый файл, а также не обеспечивается гарантированное восстановление фрагментированных файлов. При

восстановлении файла на этом уровне пользователь должен указать первую букву имени файла.

Для восстановления и защиты файлов в ОС Windows можно воспользоваться утилитой MWUNDEL. Однако в этой ОС имеется собственное средство для защиты и восстановления удаленных файлов - Корзина, являющаяся аналогом каталога SENTRY. Если дважды щелкнуть по значку Корзины, то появится окно папки со стандартным набором меню: Файл. **Правка, Вид, ?.** По команде **Свойства** меню **Файл** можно получить сведения об удаленных файлах и папках (каталогах) и настроить размер корзины для каждого логического диска. Если установить нулевое значение размера **Корзины,** то файлы будут удаляться без помещения их в **Корзину.**

Для восстановления в исходной папке файла или папки нужно выделить имя (имена) восстанавливаемого объекта (объектов) и выполнить команду Восстановить в меню **Файл.** Для удаления содержимого корзины нужно выполнить команду **Файл | Очистить корзину.**

Для защиты и восстановления файлов в среде ОС Windows95 фирма Symantec разработала в составе комплекта Norton Utilities программы Un Erase Wizardи Norton Protection.

Un Erase Wizard является мастером, предназначенным для восстановления удаленных файлов. При его использовании на экран последовательно выводятся диалоговые окна с указанием шагов, которые должны быть выполнены для восстановления файлов.

Norton Protection расширяет возможности восстановления файлов, предоставляемые Корзиной. Windows 95 не всегда помещает в Корзину файлы, удаленные из приложений или окон MS-DOS. Norton Protection помечает такие файлы как, удаленные и копирует их в особом формате в скрытую папку NProtect. Un Erase Wizardи Norton Protection подключаются по умолчанию при установке Norton Utilities.

Для обеспечения сохранности файлов на дисках и восстановления их необходимо систематически проводить комплекс профилактических мероприятий, а именно:

- выполнять дефрагментацию дисков;
- осуществлять тестирование поверхности дисков;

- контролировать объем свободной памяти на дисках;
- проверять целостность файловой структуры дисков.

Под *фрагментацией диска* понимается наличие свободных кластеров между областями диска, занятыми файлами. При сохранении новых файлов в таких кластерах может быть размещен один и тот же файл, так что он оказывается «разбросанным» в несмежных областях диска. Такое размещение информации снижает скорость доступа к файлам из-за необходимости часто перемещать магнитные головки дисководов, причем замедление работы компьютера может быть значительным. Кроме того, если файлы защищены от удаления на уровне Standard, то фрагментированные файлы нельзя восстановить.

Для ***дефрагментации*** файлов и дисков в MS-DOS можно использовать команду DEFRAG и Norton-утилиту Speed Disk (SPEEDISK). Команду DEFRAG нельзя использовать в среде Windows, так как можно потерять данные. Для дефрагментации дисков в Windows 95 используется служебная программа Disk Defragmenter.

Norton-утилита Speed Diskвыполняет те же функции, что и DEFRAG, и позволяет деф-рагментировать не только файлы, но и каталоги, а также пере разместить файлы и каталоги в начало диска. Имеются два варианта этой утилиты: для использования в MS-DOSи для использования в Windows.

Запустить утилиту Speed Diskв Windows 95 можно следующими способами:

- из окна Norton System Doctor, выбрав в меню Утилиты пункт Speed Disk;
- загрузить программу SD32.EXE из папки Norton Utilities.

При тестировании магнитных дисков выявляются ***физические*** и ***логические дефекты.*** Физические дефекты появляются вследствие механических повреждений и/или старения дискового покрытия. Логические дефекты вызывают повреждение файловой структуры. К ним относятся:

- наличие пустых кластеров, то есть таких, к которым невозможен доступ;
- наличие файлов, имеющих общие кластеры;
- повреждение каталогов и FAT;
- различие в копиях FAT. Причинами появления логических дефектов могут быть:
- внезапное отключение питания компьютера и сбои оборудования;
- деструктивные действия компьютерных вирусов. Для тестирования

магнитных дисков и восстановления информации на них могут быть использованы команда MS – DOS SCANDISK и утилита Norton Disk Doctor.

Команда SCANDISK функционирует в диалоговом и не диалоговом режиме. Файл SCANDISK.INI содержит параметры, определяющие режим работы программы SCANDISK. Он находится в одном каталоге со SCANDISK. Нерекомендуется запускать SCANDISK в среде Windows, так как это может привести к потере данных. Утилита Norton Disk Doctor (NDD) имеется в двух вариантах - для работы в среде MS-DOS и Windows. Утилита функционирует в диалоговом режиме.

Утилита Norton Disk Doctorдля Windowsможет быть запущена аналогично другим утилитам этого пакета несколькими способами:

- из окна Norton System Doctor, после выбора в меню Утилиты пункта Norton Disk Doctor,
- загрузкой программы NDD32.EXE из папки Norton Utilities.

Настройку утилиты можно производить после нажатия на кнопку Параметры в ее окне Утилиту можно настроить на автоматическую диагностику дисков при запуске Windows 95.

Комплексную проверку дисков в Windows 95 можно проводить при помощи утилиты Norton System Doctor. Она сообщает пользователю о критическом состоянии параметров вычислительной системы при помощи так называемых ***датчиков.***

Чаще всего используются следующие датчики:

- Датчик ***Целостности диска,*** непрерывно следящий за состоянием FATи структуры каталогов на выбранном устройстве, чаще всего на системном диске. При выявлении проблем Norton System Doctorпри соответствующей настройке может запустить Norton Disk Doctor для устранения ошибок во избежание повреждения файлов.
- Датчик ***Теста поверхности магнитного диска,*** непрерывно следящий за состоянием поверхности диска, который, как и датчик целостности диска, может запустить Norton Disk Doctor.
- Датчик ***Фрагментации диска,*** предназначенный для отслеживания фрагментированности диска и автоматического вызова утилиты Speed Disk, если диск окажется сильно фрагментированным.
- Датчики ***Готовности аварийного диска и Данных образа системной***

области *диска,* отслеживающие сроки создания аварийного диска и образа диска. Аварийный диск обеспечивает возможность восстановления информации после отказа компьютера. Эти датчики, зависимости от настройки, выдают предупреждение или автоматически обновляют аварийный диск и образ системной области диска.

Утилиту Norton System Doctor обычно помещают в меню Автозагрузка для автоматического запуска в начале каждого сеанса работы с Windows 95. Разумеется, ее можно запустить и другими средствами Windows.

II. Ограничение доступа к информации.

Оно обеспечивается программными и техническими средствами: *применением паролей, шифрованием файлов, уничтожением файлов* после их удаления, использованием ***электронных ключей,*** изготовлением ЭВМ в специальном *защищенном* исполнении.

Под ***ограничением доступа к информации*** *понимается исключение несанкционированного доступа к ней.*

Пароли применяются для идентификации пользователей и разграничения их прав в сети ЭВМ и для ограничения доступа пользователей, работающих на одной ЭВМ, к различным логическим дискам, каталогам и файлам. Для этих целей используются утилиты сетевых *ОС и* утилиты независимых разработчиков программных средств и встроенные средства парольной защиты приложений, в том числе систем управления базами данных, электронных таблиц и т. п.

Могут быть установлены различные уровни парольной защиты. Например, чтение диска возможно без ввода пароля, а для изменения, удаления или сохранения файла на защищенном диске пароль нужен. Парольная защита файлов не предполагает обязательное их шифрование.

Шифрование - это такое преобразование данных, в результате которого их можно прочесть только при помощи ключа. Шифрованием занимается наука, которая называется криптографией. В криптографии любой незашифрованный текст называется открытым текстом, а зашифрованные данные называются зашифрованным текстом. Современные алгоритмы шифрования представляют собой сложную математическую задачу, для решения которой без знания дешифрующего ключа требуется выполнить гигантский объем вычислений и получить ответ, возможно, через несколько лет.

В настоящее время имеются два способа цифровой криптографии: традиционная криптография и криптография **с** открытым ключом.

В *традиционной криптографии* для шифрования и дешифрования используется один и тот же ключ, основанный на каком-либо стандарте. В США, например, сегодня для шифрования используется стандарт DES (Data Encription Standard). Алгоритм шифрования с одним ключом называется ***симметричным.*** Его лучше всего использовать для шифрования файлов на жестком диске.

В *криптографии с открытым ключом* используются два различных ключа: ***открытый ключ*** - для шифрования и ***закрытый (секретный, или честный)*** - для дешифрования. Алгоритм шифрования с двумя ключами *называется* ***асимметричным.*** Такой алгоритм позволяет передавать зашифрованную информацию по компьютерным сетям. Для этого отправитель должен сначала получить от адресата его открытый ключ, а затем переслать зашифрованную открытым ключом информацию. Адресат расшифровывает ее своим закрытым ключом. Понятие «открытый ключ» означает, что ключ пересылается по сети ЭВМ, например по электронной почте, в то время как закрытый ключ таким способом не пересылается.

Теория шифрования с использованием открытого ключа была разработана Уэтфилдом Диффи и Мартином Хелманом, а трое ученых - Дональд Ривест, Эди Шамир и Лен Эдлман -создали алгоритм реализации криптографии с открытым ключом и основали затем компанию RSA Data Security.

Для ***симметричных алгоритмов,*** применяющихся в коммерческих системах, рекомендуется использовать ключ, имеющий не менее 90 двоичных разрядов. В настоящее время имеются программы шифрования, допускающие применение 128-разрядных ключей. Это означает, что если попытаться угадать ключ методом проб и ошибок, нужно перебрать 2 в 128 степени возможных значений ключей.

В *асимметричном шифровании* используются алгоритмы, отличные от симметричного шифрования. Ключи для надежной защиты информации при использовании алгоритма RSAимеют от 768 до 2048 двоичных разрядов. По расчетам криптографов, взломать защиту с 2048-разрядным открытым ключом так же трудно, как найти 128-разрядный симметричный ключ методом проб и ошибок.

В настоящее время имеются различные программные средства и аппаратно-программные комплексы защиты от несанкционированного доступа. Из программных средств следует отметить Norton-утилиты Disk Monitor (DISKMON), Diskreet (DISKREET) и Wipeinfo (WIPEINFO).

Утилита Disk Monitor выполняет следующие функции:

- уничтожение полиморфных вирусов (мутантов); защищает файлы и/или системные области дисков от несанкционированной записи;
- уничтожение полиморфных вирусов (мутантов) отображает в правом верхнем углу дисплея процесс чтения или записи на диск.

При включении ***защиты дисков*** от несанкционированной записи в память загружается резидентный модуль, который выводит на экран сообщение о попытке записи. В ответ пользователь должен разрешить или запретить запись. Такой вид защиты уменьшает вероятность разрушения информации из-за ошибочных действий пользователя, а также позволяет обнаружить возможные действия вирусов. Отображение (визуализация) процесса чтения или записи на диск обращает внимание пользователя на этот процесс, чтобы пользователь мог оценить правомерность доступа к диску.

Утилита Disk Monitor может функционировать в командном и интерактивном режиме.

Утилита Diskreet предназначена для шифрования хранимой на дисках информации. Утилита позволяет:

- шифровать файлы;
- создавать и обслуживать скрытые диски, имеющие название NDisk;
- перезаписывать (заполнять) определенным кодом или автоматически удалять исходные файлы, которые были зашифрованы (зашифрованные файлы помещаются в другое место).

При шифровании файлов используется симметричный алгоритм шифрования, то есть для шифрования и дешифрования используется только один ключ, называемый в утилите «паролем». Можно использовать два метода шифрования:

- fastproprietarymethod, разработанный автором утилиты;
- DES, являющийся стандартом правительства США.

Fastproprietarymethod является быстрым, но зато велика вероятность взлома защиты. Метод DESболее медленный, но зато обеспечивает высокую степень

защиты. Выбор метода шифрования осуществляется в режиме диалога. Утилита DISKREET может функционировать в командном и интерактивном режиме.

Для защиты локальной сети от попыток несанкционированного доступа, в том числе через глобальную сеть, например Internet, применяются специальные программные (и/или аппаратные) средства, называемые *брандмауэрами.* Среди функций, выполняемых брандмауэрами, - аутентификация пользователей и контроль за содержанием информационного потока на основе заданных правил.

Утилита Wipeinfo уничтожает ставшие ненужными файлы на дисках, так что они не могут быть восстановлены никакими средствами. Как известно, удаление файлов средствами операционной системы или оболочек не уничтожает содержимое файлов, а только делает невозможным доступ к ним. Выше было показано, как этот доступ можно восстановить. Для обеспечения секретности удаленных файлов их требуется уничтожить. Кроме того, при использовании некоторых программных продуктов данные могут быть размещены во временных файлах.

Утилита Wipeinfo может функционировать в двух режимах:

- работа с файлами;
- работа с дисками. При работе с файлами Wipeinfo производит следующие действия:
- удаляет файлы и уничтожает их содержимое или только удаляет файлы;
- полностью стирает элементы каталогов, в которых хранятся сведения об уничтожаемых файлах.

При работе с дисками Wipeinfo уничтожает:

- всю информацию на дисках;
- данные, оставшиеся в свободных кластерах дискового пространства.

Утилита Wipeinfo может функционировать в командном и диалоговом режимах. Диалоговый режим используется чаще. Утилита имеет развитую систему помощи.

Электронные ключи относятся к аппаратным средствам защиты программ и данных. Электронный ключ представляет собой специализированную заказную микросхему (чип) с площадью размером немного больше спичечного коробка. Ключ имеет два разъема; одним он подключается к параллельному порту компьютера, а другой служит для подключения принтера. При этом ключ не мешает нормальной

работе принтера. Ключ сохраняет записанную в него информацию при отключении его от компьютера. Если электронный ключ защищает программу, то последняя при ее запуске проверяет наличие «своего» ключа. Если такой ключ найден, программа выполняется, иначе она выдает сообщение об ошибке и прерывает свою работу. В защитном механизме электронного ключа может быть реализована защита файлов баз данных.

Перспективным направлением в обеспечении защиты информации в ЭВМ является применение *программно-аппаратных комплексов защиты от несанкционированного доступа.* Примером такого комплекса является DALLASLOCK3.1 и его сетевой вариант DALLASLOCK3.1 for NetWare.

Комплекс DALLASLOCK3.1 выполняет следующие функции защиты:

- обеспечение возможности доступа к компьютеру и загрузки операционной системы только по предъявлению личной электронной карты пользователя (электронного ключа) Touch Memory и вводу личного пароля;
- уничтожение полиморфных вирусов (мутантов); защиту системных файлов операционной системы;
- автоматическую и принудительную блокировку компьютера с гашением экрана дисплея на время отсутствия пользователя;
- обеспечение возможности уничтожения файлов при их удалении;
- защиту файлов пользователя от несанкционированного доступа и контроль целостности дисков;
- сохранение образа системных областей компьютера на дискете с целью их восстановления в случае разрушения системы защиты;
- разграничение полномочий пользователей по доступу к ресурсам компьютера (логическим дискам, периферийным устройствам);
- уничтожение полиморфных вирусов (мутантов); регистрацию в системных журналах всех событий по входу, выходу и работе пользователей.

Кроме того, комплекс оснащен дополнительными утилитами, расширяющими возможности защиты компьютера:

- мощная защита от вирусов. Модуль Cerber Lock, входящий в состав комплекса, обеспечивает защиту более чем от 1700 вирусов, осуществляет блокировку распространения неизвестных вирусов, лечит и восстанавливает зараженные файлы и системные области жестких магнитных дисков;

- возможность создания дополнительных защищенных логических разделов и каталогов пользователей. Данные в них защищаются при помощи индивидуального пароля пользователя;
- шифрование файлов для их надежного хранения при помощи модуля Return to Life.

*Сетевой вариант комплекса DALLASLOCK3-1 for NetWare*дополнительно обеспечивает:

- полный контроль администратором сети всех действий пользователей, работающих в локальной сети;
- возможность входа в локальную сеть только по предъявлению электронной карты Touch.Memory и вводу личного пароля.

В качестве ЭВМ, изготовленных в специальном *защищенном* исполнении, можно привести семейство ЭВМ «БАГЕТ». Эти машины обеспечивают излучение информационных сигналов на уровне естественного шума. Такая мера защиты противодействует попыткам получить дистанционный доступ к конфиденциальной информации при помощи специальной подслушивающей аппаратуры. Помимо защиты по излучению ЭВМ, предусмотрены и другие меры по защите от несанкционированного доступа:

- средства криптографической защиты;
- система разграничения доступа с электронным ключом Touch Memory;
- съемный накопитель на жестком магнитном диске.

Вопросы для самоконтроля:

1. Что такое восстановление файлов, как оно выполняется и как обеспечить возможность восстановления файлов?
2. Назовите меры защиты компьютерной информации.
3. Какие средства программно-аппаратного уровня защиты вы знаете?
4. Как устанавливать пароли на BIOS, экранную заставку и документы?
5.

Раздел 3. Трансформация бизнеса в цифровой экономике
Тема 3.3 Применения блокчейна в бухгалтерском учете

Самостоятельная работа №2 Тенденции и перспективы развития систем обработки экономической информации

Цель работы:

1. Изучить тенденции и перспективы развития систем обработки экономической информации.

2. Знать тенденции и перспективы развития экономических информационных систем.

Формируемые общие и профессиональные компетенции: ПК 7.1

Литература: [1,2,3,4,5,6], конспект

Порядок выполнения работы:

Экономическая информационная система (ЭИС) формирует информационные связи между экономическими субъектами, объединяет их в единую систему, выполняет функции по сбору, хранению, обработке и выдаче необходимой информации в процессе принятия управленческих решений, поэтому в соответствии с характером обработки информации в ЭИС на различных уровнях управления выделяются следующие типы информационных систем:

1) системы обработки данных;

2) информационные системы управления;

3) системы поддержки принятия решений.

Экономические информационные системы различаются уровнями управления (стратегический, тактический, оперативный), сферами действия (государственная, коммерческая, производственная, управленческая и пр.), специализацией (системы организационно-экономического управления, информационно-поисковые системы, системы автоматизированного обучения и др.).

Также по уровню в системе государственном управления ЭИС бывают трёх типов: отраслевые (функционируют в отраслях производственной и непроизводственной сфер, решают задачи информационного обслуживания аппарата управления соответствующих ведомств), территориальные (предназначены для выполнение управленческих функций в регионе) и межотраслевые (являются специализированными системами функциональных органов управления национальной экономикой).

Особенностями ЭИС являются: цикличность обрабатываемой ими информации, сложность производимых внутренних расчётов, динамический характер систем и их постоянное развитие, а также использование принципа системного подхода при проектировании.

Проникновение новых технологий на информационный рынок происходит через его техническую составляющую и непосредственно влияет на информационную составляющую рынка, частью которой и являются ЭИС. Современные ЭИС в силу своей природы активно впитывают новейшие технологии, при этом направленность этих использований у разных типов и видов ЭИС будет различной, что объективно обусловлено теми специфическими чертами, которые присущи каждому виду ЭИС. Следует отметить, что среди выделенных нами тенденций технология гибридных облачных вычислений является универсально востребованной практически для всех видов ЭИС, и именно на её применение будут направлены основные усилия большинства предприятий.

Характерной чертой отраслевых ЭИС является направленность на решение информационных задач экономической и управленческой деятельности предприятия для получения им прибыли в определённой отрасли народного хозяйства. Поэтому наиболее востребованными технологиями для них, помимо указанной выше универсальной технологии гибридных облачных вычислений, будут также «Принеси своё устройство» и обработка сложных событий. ОАО «Газпром», являясь по существу компанией-отраслью, обладает наиболее совершенной отраслевой ЭИС «Газпром Информ» (Газпром Информ…, 2013). Перспективы её развития в

ближайшие годы связаны с реализацией стратегии информатизации ОАО «Газпром», одной из важнейших задач которой является организация разработки, внедрения и дальнейшего сопровождения типовых информационно-управляющих систем предприятия по видам деятельности ОАО «Газпром» для дочерних обществ газового бизнеса. Поэтому упор будет делаться в первую очередь на использование гибридных облачных вычислений и концепцию «Принеси своё устройство».

Территориальные ЭИС предназначены для выполнение управленческих функций в регионе, поэтому наиболее востребованной тенденцией для них будет технология обработки сложных событий как наиболее значимая при анализе и прогнозировании различных событий регионального масштаба. Крупнейшей территориальной информационной системой (ТИС) в России является ТИС Югры (Территориальная информационная2013). Перспективы её развития связаны с повышением эффективности управления социально-экономическим развитием Ханты-Мансийского автономного округа — Югры. В данном случае планируется использовать гибридные облачные вычисления и обработку сложных событий для прогнозирования чрезвычайных ситуаций.

Межотраслевые ЭИС являются специализированными системами функциональных органов управления национальной экономикой требующими существенных вычислительных мощностей, поэтому наиболее востребованной тенденцией могут стать вычисления в оперативной памяти. Типичным примером межотраслевой ЭИС является экономическая информационная система ФГУП «Всероссийский НИИ межотраслевой информации — федеральный информационно-аналитический центр оборонной промышленности» (ФГУП «ВИМИ») (Всероссийский научно-исследовательский, 2013). Перспективы данной межотраслевой ЭИС связаны с комплексным информационным сопровождением целевых проектов развития оборонно-промышленных систем России, обеспечением эффективной реализации государственной программы вооружения и государственного оборонного заказа. Основными технологиями для данной системы могут стать гибридные облачные вычисления и вычисления в оперативной памяти.

Стоит отметить, что все три указанные выше российские ЭИС имеют достаточное финансирование, поэтому имеют возможности внедрения и других новейших технологий. Так, например, все эти ЭИС рассматривают использование технологии программно-конфигурируемых сетей уже в ближайшей перспективе. Таким образом, по нашим оценкам, на данный момент можно говорить лишь об единичных «знаковых» внедрениях, а массовое внедрение подобных технологий в краткосрочном периоде не прогнозируется, и в будущем оно будет напрямую связано с процессом их удешевления.

Другим важным примером, о котором необходимо сказать является ситуация, которая связана с процессами глобализации и особенно со вступлением России в ВТО. Так, ведущие операционную деятельность на территории России крупнейшие ТНК применяют современные ЭИС, построенные с использованием всех новейших ИКТ - технологий. Американская компания Procter&Gamble, один из лидеров мирового рынка потребительских товаров, использует ЭИС на базе SAP HANA (High Performance Analytic Appliance) (SAP, 2013), непрерывно интегрируя в неё все выходящие на рынок в виде готовых решений новейшие технологии. Это даёт компании неоспоримое преимущество при организации новых филиальных сетей по всему миру, в том числе и в России. Улучшение параметров любой технологии имеет определённые границы, которые проявляются в процессе развития технологии во времени, а также в поведении технических характеристик в

зависимости от затрат на её совершенствование. Эти границы называются технологическими пределами.

При достижении предпоследнего этапа из пяти («не новая технология») своего жизненного цикла технология приближается к своему технологическому пределу, который она достигает на этапе «устаревшая технология». При этом неизбежно появляются альтернативные (замещающие) технологии с более высокими пределами. Расстояние между параметрами результативности замещаемой и замещающей технологий, которое не может быть сокращено посредством увеличения затрат на развитие отстающей технологии называется технологическим разрывом (Technological Gap). Зрелость технологии приближает технологический разрыв.

Компании, которые научились преодолевать технологические разрывы путём лучшей организации НИОКР, кооперации с другими фирмами или иными способами, получают существенное конкурентное преимущество. После того как технологический разрыв преодолён, наступает момент, когда вкладывать средства в совершенствование новой технологии гораздо выгоднее, чем в совершенствование старой, при этом процесс замещения одной технологии другой приобретает необратимый характер.

Процесс глобализации породил новый феномен, когда глобальный технологический лидер, обладающий ключевой технологией, в процессе инновационной деятельности посредством масштабных инвестиций аккумулирует технологии схожие с базовой или иные, существенно расширяющие её основные свойства. Синергетический эффект от применения данной деятельности приводит к тому, что происходит постоянное «мгновенное» переключение лидера на более продвинутую замещающую технологию. Также происходит постоянная трансформация технологическими лидерами отраслевых стандартов данного рынка с целью его изменения и получения ещё больших выгод. В данном случае, по аналогии с «цифровым разрывом второго рода» мы можем говорить, что таким образом формируется постоянно удерживаемый разрыв, который мы предлагаем называть технологическим разрывом второго рода (Technological Gap 2). Все это приводит к тому, что новые ключевые технологии могут внедряться и использоваться только узким кругом технически продвинутых и финансово обеспеченных глобальных корпораций.

Вопросы для самоконтроля:

1. Что включает в себя понятие экономическая информационная система (ЭИС)?
2. Перечислите достоинства и недостатки экономической информационной системы (ЭИС)
3. Тенденции и перспективы развития систем обработки экономической информации.

Виды источников	Наименование рекомендуемых учебных изданий
Основные	1. Сапожникова, Н. Г. Бухгалтерский учет [Электронный ресурс] : учебник / Н. Г. Сапожникова. - М. : КНОРУС, 2020. ЭБС КноРус
Нормативные	Федеральный закон «О бухгалтерском учете» от 06.12.11г. № 402-ФЗ. 3. Указанием Банка России от 11.03.2014 № 3210-У «О порядке ведения кассовых операций юридическими лицами и упрощенном порядке ведения кассовых операций индивидуальными предпринимателями и субъектами малого предпринимательства». 4. Приказ Минфина РФ от 31.10.2000 N 94н (ред. от 08.11.2010) "Об утверждении Плана счетов бухгалтерского учета финансово-хозяйственной деятельности организаций и Инструкции по его применению" 5. Альбом новых унифицированных форм первичной учетной документации, утв. Постановлением Госкомстата России от 30 октября 1997 г. № 71а. (ред. от 21.01.2003г) 6. "Положения о порядке ведения кассовых операций и правилах хранения, перевозки и инкассации банкнот и монеты банка России в кредитных организациях на территории Российской Федерации от 29 января 2018 г. N 630-П»
Дополнительные	Методические пособия для выполнения практических работ Методические пособия для выполнения самостоятельных работ
Электронные образовательные ресурсы	12. ЭБС «Book.ru», https://www.book.ru 13. ЭБС « ЮРАЙТ»https://www.biblio-online.ru 14. ЭБС «Академия», https://www.academia-moscow.ru 15. Издательство «Лань», https://e.lanbook.com 16. Электронно-библиотечная система «Университетская библиотека онлайн»,https://www.biblioclub.ru
Периодические издания	17. Журнал Главбух. Практический журнал для бухгалтера. 18. Журнал Бюджетные организации: бухгалтерский учет и налогообложение 19. Аудиторские ведомости. Интернет-ресурсы: 1.. www. consultantru-Справочная правовая система «Консультант Плюс» 2.www. minfin.ru- Министерство Финансов. 3.www. Nalog 39. ru - Федеральная налоговая служба по Калининградской области