МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационных систем и технологий

УТВЕЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«25» 04 2018 г.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ

Методические указания к выполнению практических заданий для студентов направлений 38.04.01 Экономика и 38.04.08 Финансы и кредит

Курск 2018

УДК 004.91

Составитель Д.О. Бобынцев

Рецензент
Кандидат технических наук, доцент Сазонов С.Ю.

Информационные технологии в экономике: методические указания к выполнению практических заданий / Юго-Зап. гос. ун-т; сост.: Д.О. Бобынцев. Курск, 2018. 38 с. Библиогр.: с. 38.

Содержит методические указания к выполнению практических работ по дисциплине «Информационные технологии в экономике». Предназначен для студентов направлений подготовки «Экономика» и «Финансы и кредит».

Текст печатается в авторской редакции

Подписано в печать 25.01.18Формат 60х84 1/16.
Усл.печ. л. 2,2. Уч.-изд. л. 2. Тираж 100 экз. Заказ. 177. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

Информационные технологии - этапы их развития, виды, задачи, классификация

Информационная технология (ИТ) — совокупность технических и программных средств (инструментария), с помощью которых выполняются разнообразные операции по обработке информации во всех сферах нашей жизни и деятельности.

ИТ является наиболее важной составляющей процесса использования информационных ресурсов общества. К настоящему времени она прошла несколько эволюционных этапов, смена которых определялась главным образом развитием научно-технического прогресса, а именно появление новых технических средств (инструментария) для хранения, обработки и передачи информации.

В соответствии с существующим инструментарием (основой технологии для обработки информации) и развитием коммуникаций (связи), можно выделить следующие *этапы развития ИТ*:

§ «ручная» технология (до второй половины XIX в.): инструментарий — перо, чернильница, бухгалтерская книга; коммуникации — почтовая пересылка писем, пакетов, депеш;

§ «механическая» технология (с конца XIX в.): инструментарий — пишущая машинка, телефон, фонограф; коммуникации — почта, оснащенная более совершенными средствами доставки;

§ «электрическая» технология (40—60-е гг. XX в.): инструментарий — большие ЭВМ с соответствующим программным обеспечением, электрические пишущие машинки, копировальные аппараты, портативные магнитофоны;

§ «электронная» технология (с начала 70-х гг.): инструментарий — большие ЭВМ и создаваемые на их базе автоматизированные системы управления (АСУ), оснащенные широким спектром базовых и специализированных программных комплексов;

§ «компьютерная» или «новая» технология (с середины 80-х гг.): инструментарий — персональный компьютер с большим

количеством стандартных программных продуктов разного назначения. На этом этапе создаются системы поддержки принятия решений, имеющие встроенные элементы анализа и искусственного интеллекта для разных уровней управления. Начинается широкое использование компьютерных сетей и средств телекоммуникационной связи.

Компьютерные информационные технологии и их классификация

Компьютерная информационная технология (КИТ) — это система методов и способов сбора, регистрации, хранения, накопления, поиска, обработки и выдачи информации по запросам пользователей с помощью средств вычислительной и коммуникационной техники.

Для современных КИТ характерны:

§ диалоговый режим решения задачи с широкими возможностями для пользователя;

§ сквозная информационная поддержка на всех этапах прохождения информации на основе интегрированной базы данных, предусматривающая единую унифицированную форму представления, хранения, поиска, отображения, восстановления и защиты данных;

§ безбумажный процесс обработки документа, при котором на бумаге фиксируется только окончательный вариант документа, а промежуточные версии и необходимые данные записаны на машинные носители;

§ возможность коллективного использования документов на основе группы компьютеров, объединенных средствами коммуникаций;

§ возможность адаптивной перестройки формы и способа представления информации в процессе решения задачи.

Компьютерные информационные технологии предполагают:

§ использование пакетов прикладных программа (ППП) для решения различных задач предметной области;

§ оформление и тиражирование, рассылку и передачу информации с помощью электронной почты;

§ поиск и подготовку данных, обмен данными, оформление результатов;

§ использование различных устройств ввода/вывода информации;

§ привлечение для принятия решений технологий искусственного интеллекта;

§ широкое применение средств мультимедиа;

§ и многое другое.

Анализ рынка информационных систем и составляющих компонентов позволяет распределить КИТ на два класса: базовые и прикладные. Причем граница этого деления является условной.

Базовые КИТ — технологии, обеспечивающие решение отдельных компонент функциональных задач, а также служащие основой для формирования прикладных технологий информатизации, включают в себя:

1. Современную микроэлектронную базу средств вычислительной техники и телекоммуникаций;

2. Перспективные вычислительные средства (компьютеры нетрадиционной архитектуры, нейрокомпьютеры);

3. Технологии организации вычислительного процесса.

Можно привести следующие примеры базовых технологий:

§ технологии операционных систем, непосредственно управляющие работой средств вычислительной техники;

§ технологии архитектуры клиент/сервер, реализуемые в корпоративных сетях для коллективного доступа к информационным ресурсам вычислительных систем;

§ технологии многопроцессорной обработки, позволяющие наращивать мощность ЭВМ за счет расширения их вычислительной структуры;

§ технологии нейровычислений, реализующие отдельные виды сложной обработки информации на специально созданных программно-технических устройствах, входящих в состав ЭВМ и работающих по принципам нейронных сетей;

§ технологии автоматизации проектирования (CASE-технологии), осуществляющие разработку информационных систем, не используя для этих целей языков программирования;

§ телекоммуникационные технологии, обеспечивающие взаимодействие в сетях на основе единых стандартов;

§ технологии Intranet и Internet;

§ технологии аналого-цифровых преобразований, позволяющие преобразовывать данные из цифровой формы в аналоговый вид, что позволяет производить их компьютерную обработку;

§ технологии распознавания образов и синтеза речи, автоматизирующие процесс распознавания объектов реального мира;

§ технологии создания и распространения информации на компакт-дисках;

§ технологии криптозащиты;

§ технологии резервирования и восстановления информации;

§ технологии человеко-машинного интерфейса, обеспечивающие унификацию взаимодействия человека и ЭВМ;

§ и др.

Прикладные КИТ — технологии, формируемые на основе базовых и ориентированные на полную информатизацию объекта, т.е. комплексное решение функциональной задачи. Они реализуют типовые процедуры обработки информации в конкретной предметной области.

К прикладным КИТ можно отнести следующие технологии:

§ технологии автоматизации офиса;

§ технологии систем контроля и качества;

§ технологии систем управления запасами;

§ технологии автоматизации банковской деятельности;

§ технологии бухгалтерских систем;

§ технологии автоматизации торговли;

§ технологии издательских систем;

§ технологии машинного перевода;

§ технологии туристической деятельности;

§ и т.д.

Задание: подготовить доклад на одну из следующих тем:

1. История развития ЭВМ.

2. Современные операционные системы.
3. Распределённые приложения.
4. Технологии многопроцессорной обработки данных
5. Нейросетевые технологии.
6. CASE-средства проектирования информационных систем.
7. Технологии Intranet и Internet.
8. Технологии аналого-цифрового и цифро-аналогового преобразования.
9. Технологии распознавания образов.
10. Технологии криптозащиты.
11. Технологии резервирования и восстановления информаци
12. Технологии человеко-машинного интерфейса.

Интернет-сайты и интернет-порталы. Поисковые ИТ

Что такое **интернет-портал**? Примерно то же самое – это интернет-сайт, который содержит большое число ссылок на другие сайты Интернета. При помощи портала посетитель может направиться в любом интересующем его направлении. Это удобный интерфейс, который помогает сориентироваться в сети, найти нужную информацию по всему интернету. Помимо навигационной части интернет-портал имеет оригинальный контент – новости, обзоры, финансовые сводки и сервисную часть, которая включает в себя различные услуги – почту, форумы, информацию о погоде, доски объявлений, голосования, развлечения, и т.п.

В различных интернет-порталах эти части развиты неодинаково. Одни порталы позиционируют себя в основном как поисковые истемы, другие – информационные либо сервисные. Но каждый развивает все три направления. Набор предоставляемых порталом услуг зависит от владельца сайта, его возможностей, желания и фантазии. Все это служит одной цели – удовлетворить потребности как можно большего числа потребителей.

Интернет-порталы принято подразделять на горизонтальные и вертикальные**.**

Горизонтальные порталы, их еще называют **универсальные.** Ориентированы на максимально широкую аудиторию, предлагают разноплановый контент и имеют большой набор разнообразных сервисов. Как правило, они выстраиваются вокруг поисковых систем.

Вертикальные порталы или **порталы-ниши**. Это порталы узко тематические. Они направлены на какую-то определенную тематику или сферу деятельности и представляют интерес для пользователей сети по определенным направлениям. Среди таких тематических порталов наиболее распространены финансовые, технологические, развлекательные и религиозные ресурсы, а также это могут быть региональные порталы – сайты какого-нибудь региона, города. Как правило, такие порталы образуют вокруг себя «сообщества» («community») – более-менее постоянную группу

людей, систематически общающихся между собой в чате или форуме этого портала.

Существует **разновидности интернет-порталов**, которые в какой-то степени можно отнести к вертикальным.

Корпоративные порталы – это веб-сайты, которые предназначены для внутреннего пользования сотрудниками какой-либо компании. Они предоставляют доступ сотрудникам к корпоративной информации и к ограниченному количеству внешних веб-сайтов. В отличие от публичных, такие порталы доступны для ограниченного числа пользователей. Примером такого портала может служить сайт про строительство коттеджей.

Государственные порталы - это сайты госструктур, которые постепенно набирают вес, обзаводятся каталогами ресурсов, форумами. Они публикуют новости, экономические или политические обзоры в рамках своей специфики.

Информационные порталы – обеспечивают информационное обслуживание пользователей в определенном направлении (новости, законодательство, образование). Обновление информации на них происходит в реальном времени.

Можно выделить еще **порталы общего назначения** – они объединяют несколько тем и ориентированы на широкую аудиторию и **смешанные порталы** - они сочетают в себе функции электронной торговли и справочных сервисов.

В последнее время происходит некое размывание границы между понятиями портал и сайт. В самом деле, мы говорим, что «портал – это сайт, который…». Давайте попробуем разобраться, чем же отличается **интернет-портал** от **интернет-сайта**? Если сайт большой, у него разветвленная внутренняя структура и большое количество ссылок, может ли он называться порталом?

Для того чтобы ответить на этот вопрос, сначала выясним, что такое сайт. **Веб-сайт** (англ. Website, от web — паутина и site — «место») — это совокупность документов частного лица или организации, объединённая в компьютерной сети под одним адресом (Доменным именем или IP-адресом).

Сайты бывают разные… **Сайт-визитка** – подробная визитная карточка организации, которая содержит сведения о владельце

сайта, такие как вид деятельности, прайс-лист, история создания, контактные данные. **Интернет-каталог** - корпоративный сайт фирмы, содержит информацию об ассортименте товаров, каталог предлагаемой продукции. **Промо-сайт** – сайт о конкретном товаре, услуге, событии или бренде. Содержит исчерпывающую информацию о рекламируемом объекте, о проводимых рекламных акциях, конкурсах, викторинах и т.п. **Интернет-магазин** – сайт, позволяющий организовать процесс торговли подобно реальному магазину. Содержит каталог продукции, с помощью которого можно заказать необходимые товары. Помимо бизнес-сайтов существую **игровые сайты** – интернет ресурсы, на которых организованы он-лайн-игры.

Существуют также ресурсы для общения, такие как веб-форумы, блоги, чаты. **Форум** – это ресурс для общения посетителей веб-сайта. В отличие от **чата**, в форуме существует разделение тем и возможность общаться не в реальном времени, поэтому форум предполагает более серьезные обсуждения. Форумы часто используют для разного рода консультаций, в работе служб технической поддержки. Не уступают по популярности форуму блоги. **Блог** – это личный сайт пользователя, состоит из регулярно обновляемых записей, изображений. Блог доступен общественному просмотру и предполагает диалог, полемику между автором и читателями.

Итак, из определения видно, что каждый Веб-сайт – это узкий специалист в какой-либо сфере. Он нацелен на пользователей, которых интересует конкретный вопрос в конкретной сфере и данный сайт может удовлетворить эту потребность. Веб-сайт не отличается наличием большого числа ссылок на другие сайты Интерет. Его задача – удержать клиента, заставить его воспользоваться своими услугами.

И наоборот, Интернет-портал – специалист широкого профиля. Портал имеет все то, что характерно для обычных веб-сайтов – это одновременно и поисковая система, и множество статей на различные тематики и разнообразные ресурсы.

Главное отличие интернет-портала от интернет-сайта состоит в том, что он является путеводителем по Интернету, позволяет

определить нужное пользователю направление для поиска, помогает найти любой из профильных сайтов.

Конечно, обычный сайт может называть себя порталом (к примеру, портал про туризм konf.ru), но внутренняя его суть от этого не меняется. Интернет-портал выполняет одни функции, интернет-сайт – другие. У каждого свое предназначение, своя цель. В чем-то они пересекаются, но различия очевидны. А главное, по словам Козьмы Пруткова, «всякий необходимо причиняет пользу, употребленный на своем месте».

Задание: создать свою персональную страничку на основе типовых интернет-сервисов.

Безопасность информационных технологий

Безопасность ИС – свойство, заключающееся в способности системы обеспечить конфиденциальность и целостность информации, т.е. защиту информации от несанкционированного доступа с целью её раскрытия, изменения или разрушения.

Информационную безопасность часто указывают среди основных информационных проблем XXI в. Действительно, вопросы хищения информации, её сознательного искажения и уничтожения часто приводят к трагическим для пострадавшей стороны последствиям, ведущим к разорению и банкротству фирм и даже к человеческим жертвам. В законе Российской Федерации «Об информации, информатизации и защите информации», например, подчёркивается, что «...информационные ресурсы являются объектами собственности граждан, организаций, общественных объединений, государства» и защищать информационные ресурсы, естественно, следует, как личную, коммерческую и государственную собственность.

Все угрозы информационным системам можно объединить в обобщающие их три группы:

1. Угроза раскрытия – возможность того, что информация станет известной тому, кому не следовало бы её знать.

2. Угроза целостности – умышленное несанкционированное изменение (модификация или удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую.

3. Угроза отказа в обслуживании – возможность появления блокировки доступа к некоторому ресурсу вычислительной системы.

Средства обеспечения информационной безопасности в зависимости от способа их реализации можно разделить на следующие классы методов:

• организационные методы подразумевают рациональное конфигурирование, организацию и администрирование системы. В первую очередь это касается сетевых информационных систем, их операционных систем, полномочий сетевого администратора,

набора обязательных инструкций, определяющих порядок доступа и работы в сети пользователей;

• технологические методы, включающие в себя технологии выполнения сетевого администрирования, мониторинга и аудита безопасности информационных ресурсов, ведения электронных журналов регистрации пользователей, фильтрации и антивирусной обработки поступающей информации;

• аппаратные методы, реализующие физическую защиту системы от несанкционированного доступа, аппаратные функции идентификации периферийных терминалов системы и пользователей, режимы подключения сетевых компонентов и т.д.;

• программные методы – это самые распространённые методы защиты информации (например, программы идентификации пользователей, парольной защиты и проверки полномочий, брандмауэры, криптопротоколы и т.д.). Без использования программной составляющей практически невыполнимы никакие, в том числе и первые три группы методов (т.е. в чистом виде организационные, технологические и аппаратные методы защиты, как правило, реализованы быть не могут – все они содержат программный компонент). При этом следует иметь в виду, вопреки распространённому иному мнению, что стоимость реализации многих программных системных решений по защите информации существенно превосходит по затратам аппаратные, технологические и тем более организационные решения (конечно, если использовать лицензионные, а не «пиратские» программы). Наибольшее внимание со стороны разработчиков и потребителей в настоящее время вызывают следующие направления защиты информации и соответствующие им программно-технические средства:

1. Защита от несанкционированного доступа информационных ресурсов автономно работающих и сетевых компьютеров. Наиболее остро эта проблема стоит для серверов и пользователей сетей Интернет и интранет. Эта функция реализуется многочисленными программными, программно-аппаратными и аппаратными средствами.

2. Защита секретной, конфиденциальной и личной информации от чтения посторонними лицами и целенаправленного

её искажения. Эта функция обеспечивается как средствами защиты от несанкционированного доступа, так и с помощью криптографических средств, традиционно выделяемых в отдельный класс.

3. Защита информационных систем от многочисленных компьютерных вирусов, способных не только разрушить информацию, но иногда и повредить технические компоненты системы.

Активно развиваются также средства защиты от утечки информации по цепям питания, каналам электромагнитного излучения компьютера или монитора (применяется экранирование помещений, использование генераторов шумовых излучений, специальный подбор мониторов и комплектующих компьютера, обладающих наименьшим излучениям), средства защиты от электронных «жучков», устанавливаемых непосредственно в комплектующие компьютера и т.д.

Защита информации от несанкционированного доступа. Защита от несанкционированного доступа к ресурсам компьютера – это комплексная проблема, подразумевающая решение следующих вопросов:

- присвоение пользователю, а также и терминалам, программам, файлам и каналам связи уникальных имён и кодов (идентификаторов);
- выполнение процедур установления подлинности при обращениях (доступе) к информационной системе и запрашиваемой информации, т.е. проверка того, что лицо или устройство, сообщившее идентификатор, в действительности ему соответствует (подлинная идентификация программ, терминалов и пользователей при доступе к системе чаще всего выполняется путём проверки паролей, реже обращением в специальную службу, ведающую сертификацией пользователей);
- проверка полномочий, т.е. проверка права пользователя на доступ к системе или запрашиваемым данным (на выполнение над ними определённых операций – чтение, обновление) с целью разграничения прав доступа к сетевым и компьютерным ресурсам;
- автоматическая регистрация в специальном журнале всех как удовлетворённых, так и отвергнутых запросов к

информационным ресурсам с указанием идентификатора пользователя, терминала, времени и сущности запроса, т.е. ведение журналов аудита, позволяющих определить, через какой хост-компьютер действовал хакер или кракер, а иногда и определить его IP-адрес и точное местоположение.

Брандмауэр как средство контроля межсетевого трафика. Брандмауэр, или межсетевой экран, – это «полупроницаемая мембрана», которая располагается между защищаемым внутренним сегментом сети и внешней сетью или другими сегментами сети интранет и контролирует все информационные потоки во внутренний сегмент и из него. Контроль трафика состоит в его фильтрации, т.е. выборочном пропускании через экран, а иногда и с выполнением специальных преобразований и формированием извещений для отправителя, если его данным в пропуске было отказано. Фильтрация осуществляется на основании набора условий, предварительно загруженных в брандмауэр и отражающих концепцию информационной безопасности корпорации. Брандмауэры могут быть выполнены как в виде аппаратного, так и программного комплекса, записанного в коммутирующее устройство или сервер доступа (сервер-шлюз, прокси-сервер, хост-компьютер и т.д.). Работа брандмауэра заключается в анализе структуры и содержимого информационных пакетов, поступающих из внешней сети, и в зависимости от результатов анализа пропуска пакетов во внутреннюю сеть (сегмент сети) или полное их отфильтровывание. Эффективность работы межсетевого экрана обусловлена тем, что он полностью переписывает реализуемый стек протоколов TCP/IP, и поэтому нарушить его работу с помощью искажения протоколов внешней сети (что часто делается хакерами) невозможно. Межсетевые экраны обычно выполняют следующие функции:

- физическое отделение рабочих станций и серверов внутреннего сегмента сети (внутренней подсети) от внешних каналов связи;
- многоэтапная идентификация запросов, поступающих в сеть (идентификация серверов, узлов связи и прочих компонентов внешней сети);

- проверка полномочий и прав доступа пользователей к внутренним ресурсам сети;
- регистрация всех запросов к компонентам внутренней подсети извне; Q контроль целостности программного обеспечения и данных;
- экономия адресного пространства сети (во внутренней подсети может использоваться локальная система адресации серверов);
- сокрытие IP-адресов внутренних серверов с целью защиты от хакеров.

Криптографическое закрытие информации. Активно развиваются и внедряются криптографические компьютерные технологии, направленные на обеспечение конфиденциальности и работоспособности таких комплексных сетевых приложений, как электронная почта (e-mail), электронный банк (e-banking), электронная торговля (e-commerce), электронный бизнес (e-business). Криптографическое закрытие информации выполняется путём преобразования информации по специальному алгоритму с использованием шифров (ключей) и процедур шифрования, в результате чего по внешнему виду данных невозможно, не зная ключа, определить их содержание. С помощью криптографических протоколов можно обеспечить безопасную передачу информации по сети, в том числе и регистрационных имён, паролей, необходимых для идентификации программ и пользователей. На практике используется два типа шифрования: симметричное и асимметричное. При симметричном шифровании для шифровки и дешифровки данных используется один и тот же секретный ключ. При этом сам ключ должен быть передан безопасным способом участникам взаимодействия до начала передачи зашифрованных данных. Для осуществления симметричного шифрования применяется два типа шифров: блочные и поточные. В нашей стране для блочного шифрования информации рекомендован симметричный алгоритм, предложенный ГОСТ 28.147–89 «Системы обработки информации. Защита криптографическая». В качестве примеров поточных алгоритмов можно привести в первую очередь алгоритмы RC (RC2, RC4, RC5) корпорации RSA

Data Security (США) и алгоритмы BECTA (BECTA-2, BECTA-2M, BECTA-4) фирмы «ЛАН Крипто» (Россия).

Электронная цифровая подпись. Гражданский кодекс Российской Федерации определяет, что заключение любого юридического договора может быть осуществлено не только в письменной форме, путём составления печатного документа, подписанного сторонами, но и путём обмена документами посредством электронной связи, позволяющей достоверно установить, что документ исходит от стороны по договору. В этом случае целесообразно использовать одну из операций криптографии – цифровую электронную подпись. *Электронная цифровая подпись* – это последовательность символов, полученная в результате криптографического преобразования исходной информации с использованием закрытого ключа и позволяющая подтверждать целостность и неизменность этой информации, а также её авторство путём применения открытого ключа. При использовании электронной подписи файл пропускается через специальную программу (hash function), в результате чего получается набор символов (hash code), генерируются два ключа: открытый (public) ключ и закрытый (private) ключ. Набор символов шифруется с помощью закрытого ключа. Такое зашифрованное сообщение и является цифровой подписью. По каналу связи передаётся незашифрованный файл в исходном виде вместе с электронной подписью. Другая сторона, получив файл и подпись, с помощью имеющегося открытого ключа расшифровывает набор символов из подписи. Далее сравниваются две копии наборов, и если они полностью совпадают, то это действительно файл, сделанный и подписанный первой стороной. Для длинных сообщений с целью уменьшения их объёма (ведь при использовании электронной подписи фактически передаётся файл двойной длины) передаваемое сообщение перед шифрованием сжимается (хэшируется), т.е. над ним производится математическое преобразование, которое описывается так называемой хэш-функцией. Расшифрованный полученный файл в этом случае дополнительно пропускается через тот же алгоритм хэширования, который не является секретным. Для шифрования электронной подписи используются ранее названный алгоритм

RSA, а также DSA (национальный стандарт США) и Schnorr (алгоритм Klaus Schnorr); в России применяются алгоритмы шифрования электронной подписи по ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма» и Нотариус (Нотариус-АМ, Нотариус-S).

Защита информации от компьютерных вирусов. Компьютерным вирусом называется рукотворная программа, способная самостоятельно создавать свои копии и внедряться в другие программы, в системные области дисковой памяти компьютера, распространяться по каналам связи с целью прерывания и нарушения работы программ, порчи файлов, файловых систем и компонентов компьютера, нарушения нормальной работы пользователей. Компьютерным вирусам, как и биологическим, характерны определённые стадии существования:

- латентная стадия, в которой вирусом никаких действий не предпринимается; инкубационная стадия, в которой основная задача вируса – создать как можно больше своих копий и внедрить их в среду обитания;
- активная стадия, в которой вирус, продолжая размножаться, проявляется и выполняет свои деструктивные действия.

Сейчас существуют сотни тысяч различных вирусов, и их можно классифицировать по нескольким признакам. По среде обитания вирусы можно разделить на:

- файловые;
- загрузочные;
- файлово-загрузочные;
- сетевые;
- документные.

Файловые вирусы чаще всего внедряются в исполняемые файлы, имеющие расширения .exe и .com (самые распространённые вирусы), но могут внедряться и в файлы с компонентами операционных систем, драйверы внешних устройств, объектные файлы и библиотеки, в командные пакетные файлы (вирус подключает к такому файлу исполняемые программы, предварительно заразив их), программные файлы на

языках процедурного программирования (заражают при трансляции исполняемые файлы). Файловые вирусы могут создавать файлы-двойники (компаньоны-вирусы). В любом случае файловые вирусы при запуске программ, ими заражённых, берут на время управление на себя и дезорганизуют работу своих «квартирных хозяев».

Загрузочные вирусы внедряются в загрузочный сектор дискеты (boot-sector) или в сектор, содержащий программу загрузки системного диска (master boot record). При загрузке операционной системы с зараженного диска такой вирус изменяет программу начальной загрузки либо модифицируют таблицу размещения файлов на диске, создавая трудности в работе компьютера или даже делая невозможным запуск операционной системы.

Файлово-загрузочные вирусы интегрируют возможности двух предыдущих групп и обладают наибольшей «эффективностью» заражения.

Сетевые вирусы используют для своего распространения команды и протоколы телекоммуникационных систем (электронной почты, компьютерных сетей).

Документные вирусы (их часто называют макровирусами) заражают и искажают текстовые файлы (.doc) и файлы электронных таблиц некоторых популярных редакторов. Комбинированные сетевые макровирусы не только заражают создаваемые документы, но и рассылают копии этих документов по электронной почте (печально известный вирус «I love you» или менее навредивший вирус «Анна Курникова»).

По способу заражения среды обитания вирусы делятся на:

- резидентные;
- нерезидентные.

Резидентные вирусы после завершения инфицированной программы остаются в оперативной памяти и продолжают свои деструктивные действия, заражая следующие исполняемые программы и процедуры вплоть до момента выключения компьютера.

Нерезидентные вирусы запускаются вместе с заражённой программой и после её завершения из оперативной памяти удаляются.

Вирусы бывают неопасные и опасные. Неопасные вирусы тяжёлых последствий после завершения своей работы не вызывают; они прерывают на время работу исполняемых программ, создавая побочные звуковые и видеоэффекты (иногда даже приятные), или затрудняют работу компьютера, уменьшая объём свободной оперативной и дисковой памяти. Опасные вирусы могут производить действия, имеющие далеко идущие последствия: искажение и уничтожение данных и программ, стирание информации в системных областях диска и даже вывод из строя отдельных компонентов компьютера (жёсткие диски, Flash-чипсет BIOS, перепрограммируя его).

По алгоритмам функционирования вирусы весьма разнообразны, но можно говорить о таких, например, их группах, как:

- паразитические вирусы, изменяющие содержимое файлов или секторов диска; они достаточно просто могут быть обнаружены и уничтожены;
- вирусы-репликаторы («черви» WORM), саморазмножающиеся и распространяющиеся по телекоммуникациям и записывающие по вычисленным адресам сетевых компьютеров транспортируемые ими опасные вирусы (сами «черви» деструктивных действий не выполняют, поэтому их часто называют псевдовирусами);
- «троянские» вирусы маскируются под полезные программы (существуют в виде самостоятельных программ, имеющих то же имя, что и действительно полезный файл, но иное расширение имени; часто, например, присваивают себе расширение .com вместо .exe) и выполняют деструктивные функции (например, очищают FAT); самостоятельно размножаться, как правило, не могут;
- вирусы-невидимки (стелс-вирусы), по имени самолета-невидимки «stealth» способны прятаться при попытках их обнаружения; они перехватывают запрос антивирусной программы и мгновенно либо удаляют временно своё тело из заражённого

файла, либо подставляют вместо своего тела незаражённые участки файлов;

- самошифрующиеся вирусы (в режиме простоя зашифрованы и расшифровываются только в момент начала работы вируса);
- мутирующие вирусы (периодически автоматически видоизменяются, копии вируса не имеют ни одной повторяющейся цепочки байт), необходимо каждый раз создавать новые антивирусные программы для обезвреживания этих вирусов;
- «отдыхающие» вирусы (основное время проводят в латентном состоянии и активизируются только при определённых условиях, например, вирус «Чернобыль» в сети Интернет функционирует только в день годовщины чернобыльской трагедии).

Способы защиты от вирусов. Для обнаружения и удаления компьютерных вирусов разработано много различных программ. Эти антивирусные программы можно разделить на:

- программы-детекторы;
- программы-ревизоры;
- программы-фильтры или сторожа;
- программы-доктора или дезинфекторы, фаги;
- программы-вакцины или иммунизаторы.

Программы-детекторы осуществляют поиск компьютерных вирусов в памяти машины и при обнаружении искомых сообщают об этом. Детекторы могут искать как уже известные вирусы (ищут характерную для конкретного, уже известного вируса последовательность байтов – сигнатуру вируса), так и произвольные вирусы (путём подсчёта контрольных сумм для массива файла).

Программы-ревизоры являются развитием детекторов, но выполняющие значительно более сложную и эффективную работу. Они запоминают исходное состояние программ, каталогов, системных областей и периодически или по указанию пользователя сравнивают его с текущим. При сравнении проверяется длина файлов, дата их создания и модификации, контрольные суммы и байты циклического контроля и другие параметры.

Программы-фильтры выполняют наблюдение и выявление подозрительных, характерных для вирусов процедур в работе

компьютера (коррекция исполняемых .exe и .com файлов, запись в загрузочные секторы дисков, изменение атрибутов файлов, прямая запись на диск по прямому адресу и т.д.). При обнаружении таких действий фильтры посылают пользователю запрос о подтверждении правомерности таких процедур.

Программы-доктора – самые распространённые и популярные программы. Эти программы не только обнаруживают, но и лечат заражённые вирусами файлы и загрузочные секторы дисков. Они сначала ищут вирусы в оперативной памяти и уничтожают их там (удаляют тело резидентного файла), а затем лечат файлы и диски. Многие программы-доктора находят и удаляют большое число (десятки тысяч) вирусов и являются полифагами.

Программы-вакцины применяются для предотвращения заражения файлов и дисков известными вирусами. Вакцины модифицируют файл или диск таким образом, что он воспринимается программой-вирусом уже заражённым, и поэтому вирус не внедряется. Среди популярных и эффективных антивирусных программных средств можно выделить: *Anti Virus Toolkit Pro (AVP); McAfee VirusScan; Panda Ant ivirus; Norton AntiVirus* и др. При выборе антивирусного обеспечения следует принимать во внимание перечень и качество предоставляемых услуг. Средства антивирусной защиты должны предоставлять следующие возможности:

- Создание образа жесткого диска на внешних носителях (например, на гибких дисках или CD). В случае выхода из строя данных в системных областях жесткого диска сохраненный «образ диска» позволит восстановить если не все данные, то по крайней мере их большую часть.
- Регулярное сканирование жестких дисков в поисках компьютерных вирусов. При сканировании следует иметь в виду, что антивирусная программа ищет вирус путем сравнения кода программы с кодами известных ей вирусов, хранящихся в базе данных. Поэтому для надежной работы следует регулярно обновлять антивирусную программу.
- Контроль за изменением размеров и других атрибутов файлов. Поскольку некоторые компьютерные вирусы на этапе

размножения изменяют параметры зараженных файлов, контролирующая программа может обнаружить их деятельность и предупредить пользователя.

- Контроль за обращениями к жесткому диску. Наиболее опасные операции, связанные с работой компьютерных вирусов, обращены на модификацию данных записанных на жестком диске. Поэтому антивирусные программы могут контролировать обращения к нему и предупреждать пользователя о подозрительной активности.

Качество работы антивируса определяется его надежностью и эффективностью**.**

Задание: подготовить доклад по одной из следующих тем:

1. Алгоритмы шифрования.
2. Электронная цифровая подпись.
3. Брандмауэры.
4. Программы-детекторы.
5. Программы-ревизоры.
6. Программы-фильтры.
7. Программы-доктора.
8. Программы-вакцины.
9. Файловые вирусы.
10. Загрузочные вирусы.
11. Сетевые вирусы.
12. Документные вирусы.
13. Резидентные вирусы.
14. Нерезидентные вирусы.
15. Троянские программы.

Автоматизация текущих задач оперативного, тактического и стратегического планирования

Сегодня реализовать эффективный *финансовый менеджмент* в компании без применения программных средств невозможно. В связи с этим компания должна решить проблему, касающуюся разработки и реализации стратегии развития бизнеса вместе со стратегией развития соответствующих средств информатизации в комплексе.

Современные информационные технологии позволяют построить адекватную модель предприятия, "проиграть" различные сценарии его развития и оценить его ключевые финансовые показатели. При этом существуют два пути, по которым может идти компания в вопросах информатизации: разработка собственных программных продуктов, обеспечивающих решение задач *стратегического планирования* и управления, или приобретение готовых.

С учётом сложности описанных задач ясно, что разработка оригинальных программных систем, автоматизирующих их решение, – трудоёмкий и дорогостоящий процесс, требующий специальных знаний, поэтому для подавляющего большинства компаний эффективным решением является реализация технологий *стратегического планирования* и управления на основе готовых программных решений.

В настоящее время свои решения, относящиеся к данной области, предлагает целый ряд производителей программных средств. Одним из них является компания "*Expert Systems*", спектр решений которой по праву считается наиболее полным для автоматизации решения задач менеджмента в цепочке "диагностика – выбор *стратегии* – планирование – осуществление контроля реализации".

В настоящее время российские предприятия, вслед за всем цивилизованным миром вступили в период не просто рыночной экономики, а "информационной" экономики постиндустриального общества. Основные потребности уже удовлетворены и фирмы должны либо искать специфические потребности, либо создавать новые, или просто улучшать продукцию, создаваемую в настоящее

время. Несмотря на то, что в большинстве случаев к огорчению предприятий и радости потребителей конкуренция вытесняет слабые компании, единственный способ выжить сегодня – это использовать информацию осмысленно и быстро.

Какая же информация нужна фирмам для того, чтобы найти свое место "под солнцем"? Только принципы бухгалтерского учёта определяют фирму как независимую единицу, но в действительности она тесно интегрирована с рынком и средой. В качестве объектов самых сильных связей можно отметить потребителей, конкурентов, партнеров и инвесторов. Кроме того, на её деятельность оказывают влияние политические, экономические, социальные и технологические ситуации. Когда фирма получает информацию о потребителях, она определяет круг своих желаний и создает набор целей, которых хотела бы достичь. Информация о конкурентах, партнёрах, инвесторах даёт возможность выбрать наиболее важные цели из этого набора и определить пути реализации выбранных целей.

Однако важно не только знание внешних факторов, но также внутренних возможностей и потребностей фирмы. Фирма – это сложная взаимодействующая система собственников, менеджеров, служащих, ресурсов и технологий, и связи между всеми элементами этой системы должно быть достаточно прозрачны. Знание этих взаимосвязей, во-первых, помогает менеджерам компании осознать потенциал организации, необходимый для достижения поставленных целей, а, во-вторых, получать точную информацию о процессах, происходящих внутри предприятия. Другая важная информация касается источников возможностей, третья – внутренних процессов. Наличие адекватной информации важно не только для развития самой фирмы, но и для её контрагентов. Для того чтобы разработать эффективные информационные каналы с клиентами и партнерами, фирма должна понимать свои собственные процессы. Фирма, которая может легко обеспечить других достоверной и необходимой информацией, получает серьёзное преимущество, так как другие участники рынка также находятся в постоянном поиске достоверной информации. Потребители заинтересованы в надёжности и скорости выполнения заказа, инвесторы – в

финансовой информации относительно фирмы, партнеры – в знаниях о направлении развития фирмы; особенно важным является то, что вся эта информация должна быть получена своевременно. Поэтому получение информации извне и её предоставление другим, создаёт как дополнительные возможности, так и обусловливает возникновение новых путей для реализации этих возможностей.

Кроме того, сейчас с уверенностью можно говорить, что в XXI веке точные знания о внутренних операциях фирмы есть основа роста и выживания бизнеса. Системы моделирования и планирования ресурсов предприятия представляют собой средство ясного понимания внутренних процессов.

Однако все эти системы – это не только инструмент для получения информации, но и носитель определённых стандартов менеджмента.

Задание: выбрать программный продукт для стратегического планирования и подготовить доклад о нём.

Оценка эффективности АИТ на предприятии

В современных условиях достаточно быстро развивается рынок новых технологий управления, которые используются для предприятий самого различного профили, с разнообразными организационными структурами управления, с разной численностью работающих. Разработка и внедрение новых АИТУ требует больших единовременных затрат, эксплуатационных расходом, затрат живого труда. При обосновании целесообразности осуществления таких крупных затрат инвестор обычно требует проведения расчетов по оценке эффективности проводимых мероприятий. Для этого необходимо установить:

• факторы, действие которых обеспечивает эффективность;

• направления действия этих факторов;

• показатели для количественного измерения степени влияния данных факторов;

• методы расчета этих показателей.

Основными факторами являются повышение качества проведения вычислительных работ, повышение надежности функционирования вычислительных ресурсов, сокращение сроков создания и освоения новых информационных технологий, увеличение объема и сокращение сроков переработки информации, повышение производительности труда разработчиков и пользователей вновь созданных информационных технологий и др.

Для определения направлений действия этих факторов надо выяснить, на что влияет разработка и внедрение конкретной информационной технологии управления, а именно:

- на эффективность труда отдельных работников управления;
- эффективность управленческой деятельности подразделений;
- эффективность процесса управления при выработке конкретного управленческого решения;
- эффективность отдельного звена иерархической системы управления;
- эффективность методов управления;
- эффективность внедряемого бизнес-процесса;
- эффективность системы управления в целом.

Для оценки эффективности АИТУ требуется методика, способная продемонстрировать отдачу этой системы, чтобы убедиться, что принимаются наиболее продуктивные и экономически оправданные решения из всех возможных. При этом представляет интерес формальный подход для измерения количественной величины эффективности новой аппаратуры и программного обеспечения, корректный способ определения тех бесконечно малых неосязаемых выгод от применения информационной технологии, которые оправдывают затраты.

Необходимо использовать различные способы комбинирования количественных и качественных методов анализа эффективности. Определяющий фактор успеха - это взаимопонимание между руководством компании и руководителями информационных служб, а также согласованная методика оценки выгод, получаемых бизнесом от внедрения информационных технологий управления. Технология оценки эффективности АИТУ может быть следующей:

1) производственное подразделение, нашедшее понос приложение, готовит техническое обоснование;

2) сотрудники отдела информационных систем анализируют предложение;

3) отдел информационных систем помогает менеджерам оценить примой и косвенный эффект;

4) ожидаемый эффект подразделяется на исчисляемый (ведущий к материальной экономии) и неисчисляемый (косвенный);

5)по оценкам исчисляемых расходов и доходов производится расчет показателей, выбранных в качестве основных; неисчисляемые эффекты включаются и обоснование в виде отдельных разделов для рассмотрения высшими руководителями;

6) руководитель производственного подразделения утверждает окончательное обоснование;

7) проект передается на утверждение руководству, которое принимает решение о выделении инвестиции;

8) устанавливается дата представления отчета о реализации проекта, в котором сравниваются ожидаемые показатели с фактическими.

Сравнение различных инвестиционных проектов АИТУ (или вариантов проекта) и выбор лучшего из них рекомендуется производить с использованием различных показателей. Основными показателями общественной эффективности являются:

• чистый дисконтированный доход;
• индекс доходности;
• внутренняя норма доходности;
• срок окупаемости.

Чистый дисконтированный доход (ЧДД) определяется как сумма текущих эффектов за весь расчетный период, приведенная к начальному шагу, или как превышение интегральных результатов над интегральными затратами. Если в течение расчетного периода не происходит инфляционного изменения цен или расчет производится в базовых ценах, то величина ЧДД для постоянной нормы дисконта вычисляется по формуле:

$$\text{ЧДД} = \sum_{t=0}^{T} (R_T - З_t) \frac{I}{(I+E)^t}$$

R_t — результаты, достигаемые на t-м шаге;
$З_t$ - затраты, осуществляемые на том же шаге;
Т - горизонт расчета, равный номеру шага расчета, на котором производится ликвидация объекта;
$(R_t - З_t)$ - эффект, достигаемый на t-м шаге;
$\frac{I}{(I+E)^t}$ -коэффициент дисконтирования;
Е – норма дисконта (в относительных единицах).

При оценке эффективности инвестиционного проекта соизмерение разновременных показателей осуществляется путем приведения (дисконтирования) их ценности к начальному периоду Если показатель ЧДД инвестиционного проекта положителен, то проект является эффективным (приданной норме дисконта) и может рассматриваться вопрос о его принятии. Чем больше значение ЧДД» тем эффективнее проект. Если инвестиционный проект будет осуществлен при отрицательном ЧДД, то инвестор понесет убытки, т. е. проект неэффективен.

Па практике используют и модифицированную формулу для определения ЧДД. Для этого из состава $З_t$ исключают капиталовложении $К_t$ на t-м шаге. Сумма дисконтированных капиталовложений равна:

$$К=\sum_{t=0}^{T} K_t \frac{1}{(1+E)^t}$$

где К - дисконтированные капитальные вложения.

Тогда формула для расчета ЧДД будет иметь вид:

$$ЧДД=\sum_{t=0}^{T} (R_t - З_t^+) \frac{1}{(1+E)^t} - K,$$

где $З_t$ - затраты на t-м шаге при условии, что и них не входит капиталовложения.

Эта формула выражает, разницу между суммой приведенных эффектов и приведенной к тому же моменту величиной капиталовложений К.

Индекс доходности (ИД) представляет собой отношение суммы приведённых эффектов к величине капиталовложений:

$$ИД=\frac{1}{K}\sum_{t=0}^{T} (R_t - З_t^+) \frac{1}{(1+E)^t}.$$

Индекс доходности тесно связан с показателем ЧДД. Он строится из тех же элементов н его значение связано со значением ЧДД: если ЧДД положителен, то ИД >1, и наоборот. Если ИД> 1, то проект эффективен; при ИД < 1 проект неэффективен.

Внутренняя норма доходности (ВНД) – это норма дисконта ($Е_{вн}$), при которой величина приведённых эффектов равна приведённым капиталовложениям:

$$\sum_{t=0}^{T} \frac{R_t - З_t^+}{(1+E_{ВН})} = \sum_{t=0}^{T} \frac{K_t}{(1+E_{вн})^t}.$$

При использовании показателя ВНД следует соблюдать осторожность. Во-первых, внутренняя норма доходности не всегда имеет место. Во-вторых, уравнение может иметь больше одного решения. Первый случай весьма редок. Во втором – корректный расчет показателя ВНД несколько затруднителен, хотя и возможен. Для первого приближения к ситуации, когда простой (недисконтированный) интегральный эффект положителен, ряд авторов предлагает принимать в качестве $E_{нв}$ значение положительного корня уравнения.

Внутренняя норма доходности проекта определяется в процессе расчета и затем сравнивается с требуемой инвестором нормой дохода на вложенный капитал. Если показатель ИНД равен или больше требуемой инвестором нормы дохода на капитал,

инвестиции в данный проект оправданы, и может рассматриваться вопрос о его принятии. В противном случае инвестиции в проект нецелесообразны. Если сравнение альтернативных (взаимоисключающих) инвестиционных проектов (вариантов проекта) по показателям ЧДД и ВНД приводит к противоположным результатам, то предпочтение следует отдавать ЧДД.

Внутреннюю норму доходности модно определить по формуле, построенной по методу интерполяции:

$$E_{вн}=A\left(\frac{C}{C-D}^{(B-A)}\right)$$

где А – ставка дисконта при отрицательном значении ЧДД;
В – ставка дисконта при положительном значении ЧДД;
С – значение ЧДД при ставке дисконта А;
D - значение ЧДД при ставке дисконта В.

Метод интерполяции дает только приближенное значение внутренней нормы доходности. Чем больше расстояние между любыми двумя точками, имеющими положительный и отрицательный ЧДД, тем менее точным будет расчет показателя ВНД. Внутреннюю норму доходности можно рассчитать с помощью приложения MS EXCEL, используя команду «Подбор параметра».

Срок окупаемости – минимальный временной интервал (от начала осуществления проекта), за пределами которого интегральный эффект становится и в дальнейшем остается неотрицательным. Иными словами, это период (измеряемый в месяцах, в кварталах и годах), начиная с которого первоначальные вложения и другие затраты, связанные с инвестиционным проектом, покрываются суммарными результатами его осуществления. Результаты и затраты, связанные с осуществлением проекта, можно вычислять с дисконтированием или без него. Соответственно получается два различных срока окупаемости. Срок окупаемости рекомендуется определять с использованием дисконтирования.

При необходимости учета инфляции расчетные формулы показателей эффективности проектов должны быть преобразованы так, чтобы из входящих значений затрат и результатов было

исключено инфляционное изменение цен, т.е. чтобы величины критериев были приведены к ценам расчетного периода. При этом необходимо учитывать изменения цен за счет неинфляционных причин и осуществлять дисконтирование. Это можно выполнить введением прогнозных индексов цен и дефилирующих множителей.

Наряду с перечисленными выше критериями возможно использование и ряда других: интегральной эффективности затрат, точки безубыточности, простой нормы прибыли, капиталоотдачи и т. д. Для применения каждого из них необходимо ясное представление о том, какой вопрос экономической оценки проекта решается с его использованием и как осуществляется выбор решения.

Ни один из перечисленных критериев сам по себе не является достаточным для принятия проекта. Решение об инвестировании средств в проект должно приниматься с учетом значений всех перечисленных критериев и интересов всех участников инвестиционного проекта. Важную роль в этом решении должна играть также структура и распределение инвестиций, привлекаемых для осуществления проекта по срокам, а также другие факторы, отдельные из которых поддаются только содержательному (а не формальному) учету (например, социальные и экологические факторы, воздействующие на здоровье людей, социальная и экологическая обстановка и регионах).

Необходимо учитывать также косвенные финансовые результаты, обусловленные осуществлением проекта, изменения доходов сторонних предприятий и граждан, рыночной стоимости земельных участков, зданий и иного имущества, а также затраты на обусловленную реализацией проекта консервацию или ликвидацию производственных мощностей, потери природных ресурсов и имущества от возможных аварий и других чрезвычайных ситуаций.

Оценка предстоящих затрат и результатов при определении эффективности осуществляется в пределах расчетного периода, продолжительность которого (горизонт расчета) принимается с учетом:

- продолжительности создания, эксплуатации и (при необходимости) ликвидации объекта;
- средневзвешенного нормативного срока службы основного технологического оборудования;
- достижения заданных характеристик прибыли (массы и/или нормы прибыли и т. д.);
- требований инвестора.

Горизонт расчета измеряется числом шагов расчета. Шагом расчета при определении показателей эффективности в пределах расчетного периода могут быть месяц, квартал или год.

Затраты, осуществляемые участниками проекта, подразделяются на первоначальные (капиталообразующие), текущие и ликвидационные, которые осуществляются соответственно на стадиях строительства, функционирования и ликвидации объекта.

Для стоимостной оценки результатов и затрат могут использоваться текущие, прогнозные и дефлированные цены. Под текущими понимаются цены, заложенные и проекте без учета инфляции. На стадии технико-экономического обоснования обязательным является расчет экономической эффективности в прогнозных и дефлированных ценах (одновременно желательно производить расчеты и в других видах цен). *Прогнозная цена* — это ожидаемая цена с учетом инфляции на будущих шагах расчета. Дефлированными ценами называются прогнозные цены, приведенные к уровню цен фиксированного момента времени путем деления на общий базисный индекс инфляции.

Денежные потоки могут выражаться в разных валютах. Рекомендуется учитывать денежные потоки в тех валютах, в которых они реализуются. Для количественного измерения эффективности АИТУ целесообразно использовать метод анализа денежных потоков и показатели общественной эффективности, рассмотренные выше. Основным при расчете этих показателей является определение результатов и затрат по каждому году расчетного периода. При этом проблемным является вопрос определения результата (дохода) от внедрения и использования или продажи данной АИТУ. Можно выделить следующие подходы к определению результативности информационной технологии:

1) когда результаты эффективности производства и управления совпадают;

2) когда результат эффективности управления ниже результата эффективности производства;

3) когда определяется только результат от внедрения (продажи) информационной технологии управления;

4) когда определение эффективности новой технологии управления предполагает разработку дерева целей и их количественную оценку;

5) когда определяется результат от разработки и внедрения конкретного управленческого решения, использующего новую информационную технологию;

6) когда определяется результат деятельности управленческого персонала на всех иерархических уровнях (или отдельном уровне), использующих новую информационную технологию.

После анализа этих подходов можно выбрать показатели и определить методы их расчета для определения результата при оценке эффективности новой информационной технологии.

Учет риска при оценке эффективности автоматизированной информационной технологии управления

В настоящее время наблюдаются глубокие изменения ситуации с рисками: потенциал ущерба становится многообразнее, крупнее, сложнее, труднее предсказуемым. С точки зрения определения риска область внедрения и эксплуатации АИТУ вызывает особый интерес, так как, во-первых, электронная обработка данных охватывает широкий круг пользователей и распространяется на новые сферы повседневной жизни; во-вторых, развитие этого сектора будет иметь далеко идущие последствия; в-третьих, системы, включающие как машинный, так и человеческие компоненты, особенно сложны в отношении оценки фактора риска.

При внедрении и эксплуатации АИТУ можно выделить две основные категории рисков: первая связана с машинными компонентами, а вторая – с людьми, которые организуют работу системы и пользуются результатами этой работы. В теории экономики предприятия известно множество определений понятия

риска, отражающих как практические потребности принятия решений, так и чисто теоретические положения. Здесь важно отметить, что не все параметры риска могут быть измерены в денежном эквиваленте, а также то, что риск и связанные с ним угрозы и ущерб зависят от ситуации, уровня информированности и культурных предпосылок, т. е. отражают культурную предрасположенность общества. Это предполагает использование множества более или менее реализуемых моделей регулирования (моделей устранения рисков).

При оценке рисков, связанных с функционированием АИТУ, можно выделить три подхода, которые следует применять в комплексе:

технический подход ориентирован в основном на ущерб оборудованию обработки данных, средствам хранении и самой информации;

производственно-экономический подход нацелен на проблемы, связанные с простоем предприятия и ухудшением его деятельности;

медицинский подход ориентирован на проблемы, связанные с возможностью нанесения вреда здоровью.

Важным является вопрос об определении сторон, которые терпят убытки по рискам. Вопросы о том, кто и в какой мере несет риски (или не песет их вовсе), определяются не экономической рациональностью, а социально-культурными факторами (например, как распределяются риски при внедрении новой информационной технологии между предприятием, обществом и индивидом зависит от социально-культурного развития страны).

Материальные риски

Материальные риски охватывают широкий круг объектов, которым может быть опасен ущерб. К таким объектам относятся аппаратура для обработки данных, их носители и средства передачи; сами данные и программы, а также средства обеспечения, оборудование для утилизации отходов, здания. К этому можно добавить нанесение ущерба в работе компонентов системы. Очень разнообразен перечень возможных причин ущерба. Это могут быть

механические и химические воздействия, электромагнитные поля и излучения, компьютерные и вирусы, неправильное использование программ, искажение данных и др.

Частота возникновения ущерба для отдельных ситуаций хорошо известна, так как ведутся исследования, предметом которых является ущерб, связанный с эксплуатацией компьютеров разных фирм-производителей. Определенные события, например, пожары или удары молнии, тщательно документируются. Данные сопоставлений, распространяемые страховыми компаниями, дают первое представление об относительном значении отдельных причин ущерба. Значительно труднее эта задача решается в случае потери данных и программных ошибок. В случае материального ущерба благодаря страхованию могут покрываться (хотя бы частично) финансовые потери, а также могут приниматься меры по стимулированию профилактики ущерба.

Риски для здоровья

Эксплуатация аппаратуры для электронной обработки данных связана с большой физической и психологической нагрузкой людей, обслуживающих эту технику. Влияние ЭВМ на организм человека изучается и документируется уже давно, но взаимосвязи в этой области по своей природе значительно сложнее, чем в области машинных компонентой информационной системы. Частота нанесения вреда здоровью при работе с компьютером является предметом научных исследований.

Определение размеров ущерба тоже требует своего решения, так как отсутствуют необходимые критерии оценки для компонентов материального ущерба, а также существует проблема учета последствий от ущерба здоровью (пока учитываются только такие параметры компенсаций, как затраты на лечение или его продолжительность). Не решены вопросы социального страхования рисков, связанных с нанесением вреда здоровью (пока от предприятий только требуют строго ориентироваться на современный уровень техники безопасности).

Задание: рассчитать ЧДД, ИД и ВНД. Численные значения показателей взять у преподавателя.

Список литературы

1. Балдин, К.В. Информационные системы в экономике [Электронный ресурс] : учебник / К.В. Балдин, В.Б. Уткин. - 7-е изд. - М. : Издательско-торговая корпорация "Дашков и К", 2017. - 395 с. - Режим доступа / http://biblioclub.ru/index.php?page=book_view_red&book_id=454036.

2. Титоренко, Г.А. Информационные системы и технологии управления [Электронный ресурс] : учебник / под ред. Г.А. Титоренко. - 3-е изд., перераб. и доп. - М. : Юнити-Дана, 2015. - 591 с. - Режим доступа / http://biblioclub.ru/index.php?page=book&id=115159

3. Бухарин, С.В. Информационные системы и экономике [Электронный ресурс] : учебное пособие / С.В. Бухарин, А.В. Мельников. - Воронеж : Воронежский государственный университет инженерных технологий, 2012. - 103 с. - Режим доступа / http://biblioclub.ru/index.php?page=book_view_red&book_id=141650.

4. Абдикеева, Н.М. Корпоративные информационные системы управления [Текст] : учебник / под ред.: Н.М. Абдикеева, О.В. Китовой. - М. : ИНФРА-М, 2010. - 464 с.

Михеева, Е.В. Информационные технологии в профессиональной деятельности экономиста и бухгалтера [Текст] : учебное пособие для студентов учреждений сред. проф. образования / Е. В. Михеева, О. И. Титова. - 5-е изд., стер. - М. : Издательский центр "Академия", 2009. - 208 с.