Министерство образования Российской Федерации

Санкт-Петербургский государственный
инженерно-экономический университет

# ЭКОНОМИКО-ОРГАНИЗАЦИОННЫЕ И ПРОГРАММНО-ТЕХНИЧЕСКИЕ ВОПРОСЫ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

Сборник научных трудов

ИНЖЭКОН



Санкт-Петербург
2003

УДК 378.001.658.011.56
ББК 32.97
Э40

*Утверждено редакционно-издательским советом СПбГИЭУ*

Рецензенты:

кафедра информатики СПбГУЭФ (зав. кафедрой д-р техн. наук, проф. *В. В. Трофимов*),
д-р техн. наук, проф. *А. А. Корниенко* (ПГУПС)



Одобрено к изданию научно-техническим советом СПбГИЭУ

Э40 **Экономико-организационные** и программно-технические вопросы обработки и защиты информации: Сб. науч. тр. / Редкол.: Е. В. Стельмашонок (отв. ред.) и др. – СПб.: СПбГИЭУ, 2003. – 124 с.

ISBN 5-88996-413-5

Рассматриваются вопросы защиты информации – защита информационных сетей, СУБД; проблемы аутентификации данных, выбора экономико-математической модели системы защиты информации; технологии защиты данных в Интернете, а также теоретические и практические вопросы обработки информации и применения информационных технологий в различных сферах.

Сборник предназначен для преподавателей, аспирантов и студентов, специализирующихся в области информационных технологий и защиты информации. Подготовлен на кафедре вычислительных систем и программирования.

УДК 378.001.658.011.56
ББК 32.97

ISBN 5-88996-413-5



## Раздел I
## ЗАЩИТА ИНФОРМАЦИИ

УДК 336.441

**© В. А. Береговой**

Санкт-Петербургский государственный
инженерно-экономический университет

# ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СЕТЕЙ В БАНКОВСКОЙ СФЕРЕ

Связующим звеном между рынками товаров, услуг, капиталов (инвестиций), рабочей силы, валют, золота является рынок информации.

По оценкам экспертов, ежегодные потери от незащищенности информации в банковских и коммерческих сетях в США и странах Западной Европы составляют 100–150 тыс. долл. США. Финансово-кредитные учреждения ежегодно расходуют на обеспечение информационной безопасности 1–4% общих затрат на информатизацию своей деятельности.

С учетом российской специфики, несовершенства информационных систем можно предположить, что ежегодные потери отечественных банков превышают указанные выше суммы. Это определяет актуальность обеспечения защиты банковской коммерческой информации.

Под информационной безопасностью будем понимать защищенность информационных систем и информационных ресурсов от внешних и внутренних угроз, препятствующих эффективному использованию информации гражданами, обществом и государством.

Обеспечение информационной безопасности призвано решать следующие основные задачи: выявление, оценка и предотвращение угроз информационным системам и информационным ресурсам; защита прав юридических и физических лиц на интеллектуальную соб-

ственность, а также сбор, накопление и использование информации; защита государственной, служебной, коммерческой и личной тайны.

Угрозы информационной безопасности подразделяются на четыре основных группы: программные – внедрение «вирусов», аппаратных и программных закладок; уничтожение и модификация данных в информационных системах; технические, в том числе радиоэлектронные, – перехват информации в линиях связи; радиоэлектронное подавление сигнала в линиях связи и системах управления; физические – уничтожение средств обработки и носителей информации; хищение носителей, а также аппаратных или программных парольных ключей; информационные – нарушение регламентов информационного обмена; незаконный сбор и использование информации; несанкционированный доступ к информационным ресурсам; незаконное копирование данных в информационных системах; дезинформация, сокрытие или искажение информации; хищение информации из баз данных.

Меры по обеспечению информационной безопасности подразделяются на юридические, организационно-экономические и технологические.

Рассмотрим традиционные и обязательные правила обеспечения информационной безопасности в банковской системе в промышленно развитых странах.

1. Свод правил безопасности и его основные принципы должны быть предельно формализованы и исключать различное толкование либо возникновение правовых коллизий.

2. Сотрудники банка независимо от их должностного уровня обязаны неукоснительно соблюдать действующие правовые нормы, касающиеся сбора, хранения и обработки банковской информации.

3. Основные принципы безопасности должны неукоснительно соблюдаться всеми подразделениями банка, независимо от их местоположения, размеров, масштабов деятельности, типов используемого оборудования или материалов и т. д. Любые отклонения (исключения) от этих принципов должны оформляться специальными документами.

4. Изменение программного обеспечения и внедрение финансовых инноваций должны сопровождаться изучением и оценкой факторов уязвимости и возможных последствий для безопасности банковских информационных сетей.



5. Приобретение стандартного информационного оборудования, его адаптация или модернизация также должны анализироваться с точки зрения возможного несанкционированного проникновения в систему данных или преднамеренного блокирования информационной сети.

6. Подразделение банка, обеспечивающее активную защиту информационных сетей, осуществляет централизованный повседневный надзор над всем комплексом системы безопасности, контролирует работу соответствующих служб и деятельность каждого сотрудника в данной области.

7. Лица, ответственные за обработку информации, должны постоянно совершенствовать методы по минимизации рисков, принимать решения относительно допустимых уровней риска (на основе сопоставления потенциальных потерь от риска и расходов на его предотвращение), контролировать круг работников, имеющих доступ к конкретной информации и средствам ее обработки.

8. Пользователь информации на каждом рабочем месте, независимо от того, включен ли его компьютер в сеть, должен гарантировать конфиденциальность данных, которые он использует, обрабатывает или создает.

9. Все сотрудники, рабочие места которых включены в компьютерную сеть банка, должны иметь секретный нетривиальный персональный код пользователя, не передаваемый и не сообщаемый никому другому.

10. Безопасность банка в целом и его информационной сети в частности является частью общей культуры предприятия. Она во многом зависит от поведения и умонастроения персонала и выполняется на «уровне рефлексов».

Одной из центральных проблем становления банковской системы России является эффективность использования в практической деятельности методов управления информационными процессами средствами ее производства, накопления, обмена, анализа и переработки и эффективной информационной защиты.

УДК 50.37.23

© И. Г. Гниденко, В. В. Пономарев
Санкт-Петербургский государственный
инженерно-экономический университет
© В. В. Пономарев
ЗАО «Транзас», Санкт-Петербург

# ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ ДАННЫХ

Информационная безопасность становится неотъемлемой частью общей безопасности предприятия, обязательной составляющей обеспечения непрерывности бизнеса современных компаний и организаций.

Обеспечение безопасности требует комплексного, системного подхода, охватывающего как технологические, так и организационные аспекты.

Необходимость повышения квалификации в области информационной безопасности становится все острее по мере того, как обеспечение защиты становится все более связанным с использованием цифровых технологий.

Аутентификация (authentication) – установление подлинности имени объекта для получения им права использования программ и данных.

В процессе идентификации каждый объект получает свой идентификатор, часто являющийся ключом секретности. В соответствии с ним при аутентификации осуществляется контроль доступа и определяется аутентичность, т. е. подлинность имени объекта. В процессе аутентификации производится сравнение пароля, сообщаемого объектом с данными, содержащимися в списке зарегистрированных объектов. Если представленные сведения совпадают с имеющимися, то объект получает право работы, но только в том объеме, который ему разрешен списком полномочий. Благодаря этому предотвращается несанкционированный доступ к ресурсам системы и сети. Аутентификация является важным компонентом технологии безопасности данных.

Поскольку создание и использование информационных массивов практически всегда разделены во времени и/или в пространстве, у потребителя всегда могут возникнуть обоснованные сомнения в том, что полученный им массив данных создан нужным источником и притом в точности таким, каким он дошел до него.



Таким образом, в системах обработки информации, помимо обеспечения ее секретности, важно гарантировать следующие свойства для каждого обрабатываемого массива данных:

– подлинность – он пришел к потребителю именно таким, каким был создан источником, и не претерпел на своем жизненном пути несанкционированных изменений;

– авторство – он был создан именно тем источником, каким предполагает потребитель.

Обеспечение системой обработки этих двух качеств массивов информации и составляет задачу их аутентификации, а соответствующая способность системы обеспечить надежную аутентификацию данных называется ее аутентичностью.

До сих пор для доступа к информационной системе и к различным приложениям чаще всего применяется ввод учетной записи и пароля. Но парольная аутентификация является весьма ненадежной. Пользователи часто применяют простейший пароль, который легко можно угадать. По данным исследований, любое слово, имеющееся в словаре, становится легкой добычей хакера, вооруженного соответствующей компьютерной программой. Такие программы в считанные секунды способны перебрать колоссальное количество слов. Защитить себя от подобных атак поможет соблюдение следующих правил:

– использовать в качестве пароля слово, которого нет в словаре (например, создать его простым чередованием гласных и согласных букв) или заменить в общеизвестном слове одну из букв на цифру или какой-нибудь иной символ;

– никогда не использовать в качестве пароля информацию личного характера – она легко может быть просчитана;

– учитывать особенности системы: если программа чувствительна к регистру букв, можно комбинировать прописные буквы со строчными;

– если по каким-либо причинам пришлось открыть пароль, его следует немедленно сменить.

В последнее время в обращение входят цифровые сертификаты, позволяя обезопасить многие участки работы (электронно-цифровые подписи, кодирование и подпись документов и электронной почты, цифровая подпись программного обеспечения и т. д.).

Главная задача, решаемая с помощью цифровых сертификатов, – обеспечение целостности внешних и внутренних информационных

потоков за счет гарантии подлинности, аутентичности и целостности передаваемой информации. Цифровой сертификат является свидетельством того, что открытый ключ шифрования, который он содержит, действительно принадлежит тому, кто указан в том же сертификате. Эта связь удостоверяется сертификационным центром, где осуществляется проверка личности пользователя, и сертификат заверяется. Сертификат может быть выписан как для конечного пользователя, так и для любого объекта – рабочей станции, сервера и т. д.

С помощью цифровых сертификатов можно надежно решить проблему передачи информации, аутентификацию при доступе к корпоративной сети или конкретному приложению, к Web-ресурсам, почтовому серверу; обеспечить безопасность финансовых трансакций, проводимых через Интернет, подписывать документы электронно-цифровой подписью и т. д.

Обычно цифровой сертификат хранится на жестком диске пользователя. Следовательно, его можно изъять. То, что ключ хранится в зашифрованном виде, уменьшает риск, но не исключает его полностью. Решить проблему хранения ключа позволяют специальные аппаратные средства. Они выступают в качестве дополнительного фактора аутентификации: пользователь должен обладать устройством, на котором хранится сертификат. Часто доступ к памяти такого устройства защищен PIN-кодом, что позволяет повысить уровень безопасности аутентификации.

Наиболее распространенными из таких устройств на европейском и российском рынках являются *смарт-карты*. Основными преимуществами этих устройств, помимо их широкого распространения, являются наличие памяти и возможность реализации криптоалгоритмов. Соответственно, при выборе смарт-карты важное значение имеют следующие факторы: размер памяти; наличие PIN-кода для реализации доступа к памяти; наличие микросхемы для аппаратной реализации криптоалгоритмов; используемые алгоритмы шифрования. Основной недостаток любых смарт-карт – необходимость устройства для считывания, что значительно повышает стоимость развертывания системы аутентификации.

*Токены* – это USB-ключи размером с брелок (в технологическом и функциональном плане полностью аналогичны смарт-картам, от которых отличаются только вариантом исполнения). Эти устройства обеспечивают мобильность пользователя, так как подключаются непосредственно к порту компьютера. Некоторые модели оснащены флеш-памятью и могут использоваться в качестве USB-накопителей. Основные достоинства и недостатки этих устройств заключены в их внешнем исполнении. С одной стороны, они имеют небольшой размер и не требуют специальных считывателей. С другой стороны, на их поверхность довольно сложно нанести «опознавательные» знаки (фамилию, должность и фотографию владельца, электронную подпись и т. д.). Кроме того, USB-порт не всегда бывает доступен.

*Криптокалькуляторы* – используют метод двухфакторной аутентификации, не привязанный к цифровому сертификату пользователя. Они могут быть выполнены в виде смарт-карты, токена или собственно калькулятора и содержать генератор случайных чисел и часы, питаемые от встроенной батареи. С некоторой периодичностью устройство-аутентификатор генерирует случайное число. Пользователь, желающий подключиться к системе, должен успеть за время периода генерации набрать на обычной клавиатуре это число. Если ему удается это сделать, сервер опознает пользователя и предоставляет ему необходимые ресурсы системы. Основными недостатками этого вида устройств являются: высокая стоимость; невозможность применения при использовании цифровых сертификатов; теоретическая возможность вычисления алгоритма работы калькулятора.

В последнее время поставщики криптокалькуляторов начали предоставлять такую услугу, как передача одноразового кода по электронной почте или в виде SMS-сообщений мобильной связи. При этом уровень безопасности снижается. Однако большим преимуществом услуги является то, что пользователю в этом случае не требуются ни считыватели, ни подключение к USB-порту, ни специальное клиентское программное обеспечение, так как поддержка технологии реализована в стандартных браузерах и операционных системах.

С точки зрения процесса аутентификации все перечисленные устройства являются вполне удобными, надежными и простыми в обращении. Применение криптокалькуляторов не требует дополнительного программного обеспечения, а аутентификация осуществляется через Web-интерфейс, поэтому они очень удобны для подключения к защищенным ресурсам из «враждебной» среды без использования цифровых сертификатов. Смарт-карты и токены более целесообразно использовать, когда применение цифровых сертификатов не

ограничивается одной лишь аутентификацией: эти устройства более выгодны по соотношению цены и возможностей для безопасного хранения закрытых ключей шифрования.

УДК 50.37.23

© К. П. Голоскоков, И. А. Рогалева, Е. Б. Попов

Санкт-Петербургский государственный инженерно-экономический университет

## БЕЗОПАСНОСТЬ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

Проблема защиты компьютерных сетей от несанкционированного доступа приобрела особую остроту. Развитие коммуникационных технологий позволяет строить сети распределенной архитектуры, объединяющие большое количество сегментов, расположенных на значительном удалении друг от друга. Все это вызывает увеличение числа узлов сетей, разбросанных по всему миру, и количества различных линий связи между ними, что, в свою очередь, повышает риск несанкционированного подключения к сети для доступа к важной информации. Особенно неприятной такая перспектива может оказаться для банковских или государственных структур, обладающих секретной информацией коммерческого или любого другого характера. В этом случае необходимы специальные средства идентификации пользователей в сети, обеспечивающие доступ к информации лишь в случае полной уверенности в наличии у пользователя прав доступа к ней.

Существует ряд разработок, позволяющих с высокой степенью надежности идентифицировать пользователя при входе в систему. Среди них, например, есть технологии, идентифицирующие пользователя по сетчатке глаза или отпечаткам пальцев. Кроме того, ряд систем используют технологии, основанные на применении специального идентификационного кода, постоянно передаваемого по сети. Так, при использовании устройства SecureID (фирмы «Security Dinamics») обеспечивается дополнительная информация о пользователе в виде шестизначного кода. В данном случае работа в сети невозможна без наличия специальной карты SecureID (похожей на кредитную), которая обеспечивает синхронизацию изменяющегося кода



пользователя с хранящимся на UNIX-хосте. При этом доступ в сеть и работа в ней могут осуществляться лишь при знании текущего значения кода, который отображается на дисплее устройства SecureID. Однако основным недостатком этой и ей подобных систем является необходимость в специальном оборудовании, что вызывает неудобства в работе и дополнительные затраты.

Рассмотрим некоторые возможности обеспечения безопасности в системах: шифрование информации при передаче по каналам связи и использование надежных (достоверных, доверительных) (Trusted) систем на примере СУБД Oracle, а также система защиты от несанкционированого доступа к сети Kerberos.

Очевидные достоинства баз данных в современной среде обработки данных служат гарантией их дальнейшего развития и использования. Контроль доступа в этой области важен ввиду колоссальной концентрации информации.

В настоящий момент «хребтом» базовых систем обработки информации во многих больших организациях является локальная сеть, которая постепенно занимает такое же место и в фирмах меньшего размера. Растущая популярность локальных сетей требует соответствующей защиты информации, но исторически они были спроектированы как раз не для разграничения, а для облегчения доступа и коллективного использования ресурсов. В среде локальных сетей в пределах здания или района (городка) сотрудник, имеющий доступ к физической линии, может просматривать данные, не предназначенные для него. В целях защиты информации в различных комбинациях используются контроль доступа, авторизация и шифрование информации, дополненные резервированием.

Шифрование данных традиционно использовалось правительственными и оборонными департаментами, но в связи с изменением потребностей и некоторые наиболее солидные компании начинают использовать возможности, предоставляемые шифрованием для обеспечения конфиденциальности информации.

Финансовые службы компаний (прежде всего, в США) представляют важную и большую пользовательскую базу, и часто специфические требования предъявляются к алгоритму, используемому в процессе шифрования. Опубликованные алгоритмы, например DES, являются обязательными. В то же время, рынок коммерческих систем не всегда требует такой строгой защиты, как правительственные или

оборонные ведомства, поэтому возможно применение продуктов и другого типа, например PGP (Pretty Good Privacy).

Устойчивость к искажению данных обеспечивается следующим образом.

1. Криптографически защищенная контрольная сумма в каждом пакете SQL* Net обеспечивает защиту от модификации данных и замены операции.

2. При обнаружении нарушений операции незамедлительно автоматически завершаются.

3. Информация обо всех нарушениях регистрируется в журнале.

Наряду с этим обеспечивается многопротокольная перекодировка данных, т. е. полностью поддерживается Oracle Multiprotocol Interchange, при работе с зашифрованной сессией можно начинать работу с одним сетевым протоколом, а заканчивать с другим, при этом не требуется дешифрование или перешифрование информации. SNS полностью поддерживается сквозными шлюзами Oracle Transparent Gateways и процедурными шлюзами Oracle Procedural Gateways, которые дают возможность организовывать полностью зашифрованные сессии клиент-сервер к отличным от Oracle источникам данных, включая Adabas, CA-Datacom, DB2, DRDA, FOCUS, IDMS, IMS, ISAM, MUMPS, QSAM, Rdb, RMS, SAP, SQL/DS, SQL/400, SUPRA, Teradata, TOTAL, VSAM и др.

SNS работает со всеми основными протоколами, поддерживаемыми SQL* Net, включая AppleTalk, Banyan, DECnet, LU6.2, MaxSix, NetBIOS, SPX/IPX, TCP/IP, X.25 и др.

Это означает, что при организации связи клиент-сервер используется новый протокол установления связи, в котором применяется сеансовый ключ, пригодный только для единственной попытки соединения с базой данных и используемый в качестве ключа для шифрования пароля, прежде чем он будет передан клиентам. Oracle-сервер находит зашифрованный пароль для этого пользователя и использует его в качестве ключа, которым он зашифровывает сеансовый ключ. Затем сервер пересылает этот зашифрованный сеансовый ключ клиенту. Клиент шифрует (применяя тот же самый односторонний алгоритм, который используется сервером) пароль, введенный пользователем, и с его помощью дешифрует зашифрованный сеансовый ключ. Этот зашифрованный пароль затем передается через сеть серверу. Сервер дешифрует пароль и затем зашифровывает его, используя односторонний алгоритм сервера; результат этих вычислений сверяется со значением, хранимым в словаре данных. Если они совпадают, клиенту предоставляется доступ. Такой подход реализуется как в соединениях типа клиент-сервер, так и сервер-сервер, где сеансы устанавливаются через так называемые полномочные звенья баз данных (звенья баз данных без вложенных имен пользователей и паролей).



Многие производители сетевого и телекоммуникационного оборудования обеспечивают поддержку работы с Kerberos в своих устройствах.

Следует, однако, отметить, что использование Kerberos не является решением всех проблем, связанных с попытками несанкционированного доступа в сеть (например, он бессилен, если кто-либо узнал пароль пользователя), поэтому его наличие не исключает других стандартных средств поддержания соответствующего уровня секретности в сети.

Ни одна компьютерная система защиты информации не является абсолютно безопасной. Однако адекватные меры защиты значительно затрудняют доступ к системе и снижают эффективность усилий злоумышленника (отношение средних затрат на взлом защиты системы и ожидаемых результатов) так, что проникновение в систему становится нецелесообразным. Ключевым элементом в системе безопасности является администратор системы.

УДК 50.37.23

**© О. Д. Мердина**
Санкт-Петербургский государственный инженерно-экономический университет

**© А. Е. Фарафонов**
ООО «Берег», Санкт-Петербург

## АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ СУБД[1]

В последние годы в нашей стране наблюдается серьезный интерес к вопросам создания и внедрения систем, призванных удовлетво-

[1] Данная статья поддержана грантом Министерства образования РФ по фундаментальным исследованиям в области гуманитарных наук ГО2-4.1-15.

рять информационные и аналитические потребности коммерческих предприятий. Корпоративные информационные системы, предназначенные для сопровождения установившихся бизнес-процессов, в настоящее время уже являются необходимым условием для эффективного ведения бизнеса, поскольку автоматизация основных операций позволяет существенно снизить их стоимость и повысить качество обслуживания клиентов, а накопленная за время функционирования системы информация позволяет аналитическим отделам вырабатывать качественные прогнозы маркетингового характера.

Данные информационные системы (ИС) накапливают и обрабатывают существенные объемы коммерческой информации, которая в случае утечки может быть использована во вред компании-владельцу в условиях ожесточающейся конкурентной борьбы. Это обуславливает необходимость рассматривать коммерческую информацию как объект защиты и требует при разработке ИС реализации определенных мер, направленных на недопущение несанкционированного доступа к данным.

Существуют четыре действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация, утечка и уничтожение. Эти действия являются базовыми для дальнейшего рассмотрения.

Придерживаясь принятой классификации, будем разделять все источники угроз на внешние и внутренние.

Источниками внутренних угроз являются:

– сотрудники организации;

– программное обеспечение;

– аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

– ошибки пользователей и системных администраторов;

– нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации;

– ошибки в работе программного обеспечения;

– отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся: компьютерные вирусы и вредоносные программы; организации и отдельные лица; стихийные бедствия.

Формами проявления внешних угроз являются:

– заражение компьютеров вирусами или вредоносными программами;



– несанкционированный доступ (НСД) к корпоративной информации;

– информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;

– действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;

– аварии, пожары, техногенные катастрофы.

Все перечисленные виды угроз (формы проявления) можно разделить на умышленные и неумышленные.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации: информационные, программные, физические, радиоэлектронные и организационно-правовые.

К информационным угрозам относятся:

– несанкционированный доступ к информационным ресурсам;

– незаконное копирование данных в информационных системах;

– хищение информации из библиотек, архивов, банков и баз данных;

– нарушение технологии обработки информации;

– противозаконный сбор и использование информации;

– использование информационного оружия.

К программным угрозам относятся:

– использование ошибок и «дыр» в ПО;

– компьютерные вирусы и вредоносные программы;

– установка «закладных» устройств;

К физическим угрозам относятся:

– уничтожение или разрушение средств обработки информации и связи;

– хищение носителей информации;

– хищение программных или аппаратных ключей и средств криптографической защиты данных;

– воздействие на персонал.

К радиоэлектронным угрозам относятся:

– внедрение электронных устройств перехвата информации в технические средства и помещения;

– перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К организационно-правовым угрозам относятся:

– закупки несовершенных или устаревших информационных технологий и средств информатизации;

– нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере.

Для создания эффективной системы защиты информации необходимо учитывать вероятность проявления всех видов угроз. Однако из всего многообразия представленных выше угроз для нас наибольший интерес представляют информационные и программные угрозы, а также методы и средства защиты информации от этих видов угроз.

С точки зрения защиты информации, самым важным звеном любой информационной системы является хранилище данных, поскольку все остальное восстанавливается относительно просто и быстро. Средства и системы защиты данных в СУБД достаточно гибки и разнообразны, при грамотном подходе они позволяют построить систему защиты высокой степени надежности.

Современные СУБД, такие как Oracle и MS SQL Server, обладают широким набором встроенных средств защиты от простейших идентификации и аутентификации до разделения пользователей (и данных) на группы и уровни, протоколирования различных событий в системе, установки расписаний – когда, для кого и с каких станций разрешен (запрещен) доступ и т. п. В СУБД предусмотрены следующие механизмы защиты данных:

*Сопровождение пользователей:*

– домены защиты пользователей – пользователи имеют доступ только к той области данных, которая необходима им для работы;

– привилегированные пользователи – пользователи разделены по привилегиям, привилегии определяют глубину доступа и права пользователей по доступу к информации (чтение, модификация, удаление и т. п.);

– способы аутентификации пользователей. Создание новых пользователей, сопровождение паролей в сервере Oracle: ресурсные ограничения, включение парольной системы, блокирование входа пользователей в систему, срок действия паролей и его истечение,



хронология изменений паролей, проверка сложности паролей, установки ресурсных ограничений парольной системы, явное блокирование входа пользователей в систему, шифрование паролей, надежность парольной системы.

*Сопровождение привилегий:*

– типы привилегий и уровень детализации доступа;

– использование представлений для дополнительного ограничения доступа;

– процедуры с правами вызывающего;

– механизмы реализации дискреционных правил разграничения доступа.

*Сопровождение ролей:* создание ролей, предоставление ролей, включение и отключение ролей, вывод информации о ролях, защищенные роли приложений.

*Виртуальные частные базы данных:* контекст приложения, детальный контроль доступа.

*Сопровождение меток безопасности:*

– механизмы реализации мандатных правил разграничения доступа;

– требования к реализации мандатного принципа контроля доступа;

– метки безопасности;

– использование Oracle Policy Manager для администрирования меток и авторизации;

*Аудит системы:* журнал аудита; включение и отключение аудита, проверка параметров и журнала аудита, настройка аудита, защита журнала аудита, выполнение аудита с помощью триггеров базы данных.

Кроме того, в СУБД Oracle и MS SQL Server реализована многоуровневая система резервного копирования (BackUp). Она позволяет создавать резервные копии различного масштаба – от базы данных в целом до состояния отдельной записи отдельного поля на протяжении ее нескольких модификаций.

Все эти средства в комплексе при грамотном администрировании позволяют создать систему защиты информации, хранимой в базе данных, высокой степени эффективности.

УДК 50.37.23

© С. А. Михальчук, Е. В. Стельмашонок

Санкт-Петербургский государственный инженерно-экономический университет

# УПРАВЛЕНИЕ ПАРАМЕТРАМИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ВЕРОЯТНОСТНО-СТАТИСТИЧЕСКОЙ МОДЕЛИ[1]

Активное внедрение автоматизированных информационных систем в различные области профессиональной деятельности остро ставит перед предприятиями, организациями, фирмами вопросы обеспечения целостности, конфиденциальности и доступности информационных ресурсов. Построение эффективной системы защиты информации опирается на экономически обоснованный выбор средств защиты, требующих значительных материальных затрат.

Экономическое обоснование выбора средств защиты требует количественных оценок. Сложность такой оценки обуславливает необходимость разработки адекватных математических моделей и применения специальных математических методов.

Потеря от угроз информации может быть выражена суммой стоимости возможного ущерба от проявления угроз и стоимости ресурсов, вложенных в защиту. Допустимым размер затрат на защиту будет таким, который обеспечивает уровень защищенности, равный минимуму общих потерь. Стоимость ущерба определяется вероятностью проявления различных угроз информации и стоимостью той информации, защищенность которой может быть нарушена. Стоимость защиты зависит от вероятности угроз и требований к защите, которые, в свою очередь, определяются стоимостью (важностью) обрабатываемой информации. Показателем возможного ущерба при нарушении защищенности информации можно считать сумму потерь (недобора прибыли) от получения злоумышленником защищенной информации. Так как определение такого естественного показателя крайне затруднительно и подходы к оценке ущерба носят сугубо эмпирический характер, может быть полезен описываемый подход.

[1] Данная статья поддержана грантом Министерства образования РФ по фундаментальным исследованиям в области гуманитарных наук ГО2-4.1-15.



В простейшем случае показатель возможного ущерба, являющийся функцией многих переменных, определен при значении параметров, приближающихся к рациональным. В этой области значений параметров функция, как правило, обладает свойством локальной линейности. Это позволяет определить коэффициенты в линейном разложении функции в разных точках этой области и статистически оценить возможные погрешности (требования к точности оценки) параметров в зависимости от заданной (допустимой) точности расчета показателя возможного ущерба.

В работе С. А. Михальчука, О. Д. Мердиной, Е. В. Стельмашонок[1] сформулирован подход к выбору значимых параметров экономико-математической модели системы защиты информации. Развивая этот подход, удалось более точно определить требования к возможным погрешностям задания значений параметров модели в зависимости от заданной (допустимой) точности расчета показателя возможного ущерба.

Пусть функция

$$y = f(\overline{X}),$$

$$\overline{X} = (x_1, x_2, ..., x_n) \in \Omega \subset R^n, \quad \Omega = \begin{Bmatrix} 0 \le x_1 \le 1 \\ \dots\dots\dots\dots \\ 0 \le x_n \le 1 \end{Bmatrix} \tag{1}$$

задает экономические показатели функционирования системы, причем в результате неточной оценки параметров системы вместо набора параметров $\overline{X}$ поступает набор $\overline{X}^1$:

$$\overline{X}^1 = \overline{X} + \Delta\overline{X}, \tag{2}$$

что приводит к погрешности в определении значения $f(\overline{X})$, равной

$$\Delta y = f(\overline{X}^1) - f(\overline{X}). \tag{3}$$

Предположим, что $f(\overline{X})$ локально-линейна, т. е. в некоторой окрестности любой точки $\overline{X^*}$ функцию можно считать линейной:

[1] *Михальчук С. А., Мердина О. Д., Стельмашонок Е. В.* Подход к выбору значимых параметров экономико-математической модели системы защиты информации // Современные информационные технологии в экономике и образовании: Сб. науч. тр. СПб.: СПбГИЭУ, 2001. С. 3–8.

$$f(\overline{X}) = f(\overline{X}^*) + \sum_{t=1}^{n} U_t (X_t - X_t^*), \qquad (4)$$

и таким образом

$$\Delta y = \sum_{t=1}^{n} U_t \Delta X_t. \qquad (5)$$

В работе [1] дается метод определения коэффициентов $U_t$ для таблично и алгоритмически заданных функций (для аналитически заданных функций $U_t$ есть частная производная $f(\overline{X})$ по $X_t$). При этом предлагается $K$ раз случайным образом выбирать из $\Omega$ точки $\overline{X^*}$ и получать $K$ наборов коэффициентов:

$$U_{1,q}^*, U_{2,q}^*, \ldots, U_{n,q}^*, \quad q = 1, 2, \ldots, k. \qquad (6)$$

Принимая, что каждый коэффициент $U_t$ в выражении (5) случайная величина, можно считать погрешность $\Delta y$ случайной функцией случайных аргументов $U_t$.

Оценку математического ожидания дисперсии случайных величин $U_t$ можно получить по формулам

$$M(U_t) = \frac{\sum_{q=1}^{k} U_{tq}^*}{K},$$

$$D(U_t) = \frac{\sum_{q=1}^{k} (U_{tq}^* - M(U_t))^2}{K-1}.$$

Тогда математическое ожидание и дисперсия погрешности $\Delta y$ могут быть вычислены по формулам

$$M(\Delta y) = \sum_{t=1}^{n} M(U_t) \Delta X_t,$$

$$D(\Delta y) = \sum_{t=1}^{n} D(U_t) \Delta X_t^2.$$

Известный из практики факт (имеющий свое теоретическое подтверждение в центральной предельной теореме теории вероятностей), что случайная величина, являющаяся суммой многих случайных величин (при некоторых несущественных ограничениях), имеет распределение, близкое к нормальному, позволяет допустить, что $\Delta y$ как сумма случайных величин распределена по нормальному закону

$$P(\Delta y) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(\Delta y - a)^2}{2\sigma}}$$

с параметрами $a = M(\Delta y)$, $\sigma = \sqrt{D(\Delta y)}$.

Вероятность того, что случайная величина $\Delta y$ отклонится от $M(\Delta y)$ не более, чем на заданное значение $\varepsilon > 0$ равна

$$P(|\Delta y - M(\Delta y)| < \varepsilon) = 2\phi\left(\frac{\varepsilon}{\sigma}\right),$$

где $\phi(X)$ – функция Лапласа

$$\phi(X) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{z^2}{2}} dz.$$

Таким образом, при заданных погрешностях параметров $\Delta X_t$ погрешность показателя возможного ущерба $\Delta y$ можно приближенно определять по простой формуле

$$\Delta y = \sum_{t=1}^{n} M(U_t) \Delta X_t.$$

При этом ошибка не будет превосходить $\varepsilon$ с вероятностью $2\phi\left(\frac{\varepsilon}{\sigma}\right)$.

Значимость (степень влияния на показатель ущерба) отдельных параметров $X_t$ в экономико-математической модели прямо пропорциональна коэффициентам $M(U_t)$.

Это позволяет расположить параметры $X_t$ в порядке убывания их значимости (т. е. по значениям $M(U_t)$), причем каждый параметр $X_t$ будет вносить в погрешность $\Delta y$ свою долю, равную $M(U_t)\Delta X_t$. Например, если модель нуждается в упрощении, и мы хотим отказаться от учета некоторых малозначимых параметров, то можно их заменить в модели на константы (на среднее значение параметров $\Delta X_t = 0{,}5$), при этом вклад отсутствующих параметров в погрешность $\Delta y$ будет равен $M(U_t)\Delta X_t$ от каждого параметра.

УДК 004.056.5

© Д. Г. Николаев

Санкт-Петербургский государственный
инженерно-экономический университет

# ВОЗМОЖНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ. МОДЕЛЬ БЕЗОПАСНОСТИ БЕЛЛА–ЛА ПАДУЛА

На сегодняшний день, по оценкам западных специалистов, утечка 20% информации, составляющей коммерческую тайну, в 60 случаях из 100 приводит к банкротству фирмы. Ни одна даже самая крупная фирма США не может просуществовать более трех суток, если ее конфиденциальная информация станет общедоступной. Поэтому защита от утечки коммерческой информации является залогом успешной деятельности любого предприятия.

Один из важнейших аспектов проблемы обеспечения безопасности компьютерных систем – определение, анализ и классификация возможных угроз безопасности.

Под угрозой (вообще) обычно понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Угрозой интересам субъектов информационных отношений будем называть потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты автоматизированной системы (АС) может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

Основными видами угроз безопасности АС являются:

– стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т. п.);

– сбои и отказы оборудования (технических средств);

– последствия ошибок проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т. п.);

– ошибки эксплуатации (пользователей, операторов и другого персонала);

– преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т. п.).



Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные) (рис. 1).

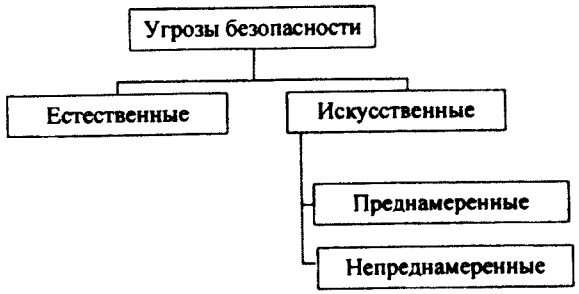



Рис. 1. Возможные угрозы безопасности

*Естественные угрозы* – это угрозы, вызванные воздействиями на АС, и ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека.

*Искусственные угрозы* – это угрозы АС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

– непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т. п.;

– преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к АС могут быть внешними или внутренними (компоненты самой АС – ее аппаратура, программы, персонал).

Чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

Защищать компоненты АС необходимо от всех видов воздействий: от преднамеренных действий злоумышленников, ошибок персонала и пользователей, ошибок в программах, сбоев и отказов технических средств, стихийных бедствий и аварий.

Одна из первых моделей безопасности – и впоследствии наиболее часто используемая – была разработана Дэвидом Беллом и Леонардо Ла Падула для моделирования работы компьютера.

Рассмотрим систему из двух файлов и двух процессов (рис. 2). Один файл и один процесс являются несекретными, другой файл и процесс – секретными.

Простое правило безопасности предотвращает чтение секретного файла несекретным процессом. Оба процесса могут читать и записывать данные в несекретный файл. Однако легко может произойти нарушение правил управления доступом, если секретный процесс считает информацию из секретного файла и запишет ее в несекретный файл. Это эквивалентно неавторизованному уменьшению класса доступа информации, хотя при этом не изменяется класс доступа ни одного файла.


Рис. 2. Модель безопасности

Когда процесс записывает информацию в файл, класс доступа которого меньше, чем класс доступа процесса, имеет место так называемый процесс записи «вниз». Ограничение, направленное на исключение нисходящей записи, получило в модели Белла–Ла Падула название **-свойства* или *свойства ограничения*.

Таким образом, модель многоуровневой безопасности имеет два основных свойства:

– простая безопасность: субъект может только читать объект, если класс доступа субъекта доминирует над классом доступа объекта, другими словами, субъект может читать «вниз», но не может читать «вверх»;

– свойство ограничения: субъект может только записать в объект, если класс доступа субъекта превосходит класс доступа объекта. Субъект может записывать «вверх», но не может записать «вниз».



Процесс не может ни читать объект с высшим классом доступа (свойство простой безопасности), ни записать объект с низшим классом доступа (*-свойство или свойство ограничения) (рис. 3).

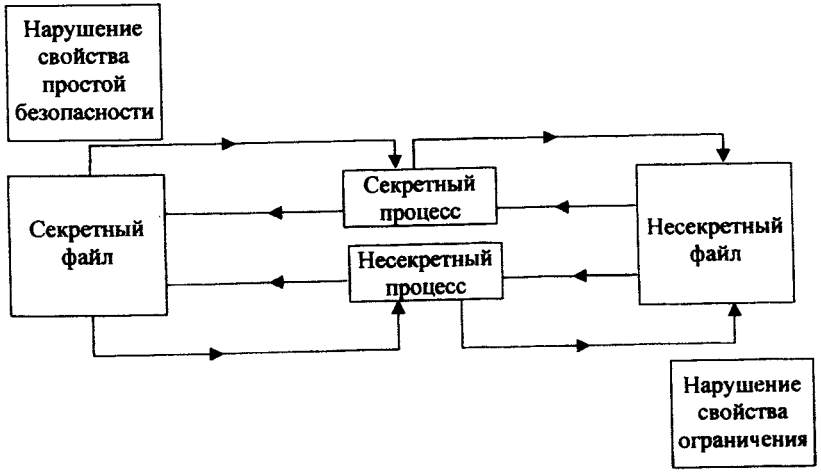



Рис. 3. Многоуровневая модель безопасности

При формализации многоуровневого управления безопасностью модель Белла–Ла Падула определяет структуру класса доступа и устанавливает упорядочивание отношений между классами доступа (доминирование). Кроме того, определяются два уникальных класса доступа: SYSTEM HIGH, который превосходит все остальные классы доступа, и SYSTEM LOW, который превосходят все другие классы. Изменения классов доступа в рамках модели Белла–Ла Падула не допускаются.

Управление доступом в модели Белла–Ла Падула происходит как с использованием матрицы управления доступом, так и с использованием меток безопасности и ранее приведенных правил простой безопасности и свойства ограничения.

В дополнение к имеющимся режимам доступа чтения и записи матрица управления доступом включает режимы добавления, исполнения и управления, причем последний определяет, может ли субъект передавать другим субъектам права доступа, которыми он обладает по отношению к объекту.

Управление при помощи меток безопасности усиливает ограничение предоставляемого доступа на основе сравнения атрибутов класса доступа субъектов и объектов.

В модели Белла–Ла Падула определено около двадцати функций (правил операций), выполняемых при модификации компонентов матрицы доступа, при запросе и получении доступа к объекту (например, при открытии файла), создании и удалении объектов; при этом для каждой функции доказывается сохранение ею, в соответствии с определением, безопасного состояния. Лишь немногие разработки безопасных систем использовали функции, предложенные Беллом и Ла Падула, чаще использовались собственные функции, разработанные на основе функций модели Белла–Ла Падула. Поэтому в настоящее время, когда говорят о модели Белла–Ла Падула, имеются в виду только простое условие безопасности и свойство ограничения, а не функции, составляющие основу модели, и их доказательства.

Рассмотренная модель является самой первой и самой простой моделью безопасности, но сегодня требования к безопасности существенно повысились, что стимулирует появление новых, актуальных решений в этой области.

УДК 004.056.378.09

© Д. Г. Николаев, О. Б. Кузнецова

Санкт-Петербургский государственный инженерно-экономический университет

## ОСОБЕННОСТИ ЗАЩИТЫ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ В ЦЕНТРАХ ДОВУЗОВСКОГО ОБРАЗОВАНИЯ

Бурное развитие средств вычислительной техники открыло перед человечеством небывалые возможности по автоматизации умственного труда и привело к созданию большого числа разного рода автоматизированных информационных и управляющих систем, к возникновению принципиально новых так называемых информационных технологий.

Современный мир находится на таком этапе своего развития, который специалисты определяют как «информационное общество». Это значит, что во всех сферах деятельности (а тем более в коммерческой деятельности) на первый план выходит информация, а следовательно, и процессы, связанные с ее получением, обработкой и использованием. Информация стала определяющим ресурсом для успешной деятельности любого предприятия. Именно поэтому защита от утечки коммерческой информации играет важную роль в обеспечении безопасности работы фирм.



Коснулась эта проблема и сферы образования, в частности, деятельности структур, реализующих программы довузовского образования, – Центров довузовского образования (ЦДО). Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах, наносят серьезный материальный и моральный ущерб ЦДО, участвующим в процессах автоматизированного информационного взаимодействия.

Жизненно важные интересы этих субъектов, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их безопасности, экономических, и других сторон деятельности, конфиденциальная коммерческая и персональная информация была бы постоянно легко доступна и в то же время надежно защищена от неправомерного ее использования: нежелательного разглашения, фальсификации, незаконного тиражирования или уничтожения.

Как показывает практика, большинство автоматизированных систем обработки информации, функционирующих в ЦДО, в общем случае представляют собой территориально распределенные системы интенсивно взаимодействующих (синхронизирующихся) между собой по данным (ресурсам) и управлению (событиям) локальных вычислительных сетей (ЛВС) и отдельных ЭВМ.

В распределенных автоматизированных системах возможны все «традиционные» для локально расположенных (централизованных) вычислительных систем способы несанкционированного вмешательства в их работу и доступа к информации. Кроме того, для них характерны и новые специфические каналы проникновения в систему и несанкционированного доступа к информации.

В качестве возможных нежелательных воздействий на компьютерные системы, которые могут возникнуть при работе ЦДО, можно рассмотреть следующие:

– преднамеренные действия злоумышленников;

– ошибочные действия обслуживающего персонала и пользователей системы;

– проявления ошибок в ее программном обеспечении;

– сбои и отказы оборудования;

– аварии и стихийные бедствия.

В качестве защищаемых объектов должны рассматриваться информация и все ее носители (отдельные компоненты и автоматизированная система обработки информации в целом).

Обеспечение безопасности вычислительной системы предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также для попыток хищения, модификации, выведения из строя или разрушения ее компонентов, т. е. защиту всех компонентов системы: оборудования, программного обеспечения, данных (информации) и ее персонала.

Исследования проблемы обеспечения безопасности компьютерных систем ведутся как в направлении раскрытия природы явления, заключающегося в нарушении целостности и конфиденциальности информации, дезорганизации работы компьютерной системы, так и в направлении разработки конкретных практических методов и средств их защиты. Серьезно изучается статистика нарушений, вызывающие их причины, личность нарушителей, суть применяемых нарушителями приемов и средств, используемые при этом недостатки систем и средств их защиты, обстоятельства, при которых было выявлено нарушение, и другие вопросы.

Обращение к теме защиты коммерческой информации в ЦДО вызвано отсутствием необходимых основ обеспечения защиты информации в современных условиях. Имеются веские основания полагать, что применяемые в настоящее время в ЦДО отечественные системы обработки информации не могут обеспечить достаточную степень безопасности деятельности подобных центров, участвующих в процессе информационного взаимодействия, и не способны в необходимой степени противостоять разного рода воздействиям с целью доступа к коммерческой информации.

Таким образом, возникает острая необходимость разработки новых (улучшенных) моделей защиты коммерческой информации, необходимой для работы и принятия решений в ЦДО.



УДК 50.37.23

© Э. А. Пиль

Петербургский государственный
университет путей сообщения

# ЗАЩИТА КОММЕРЧЕСКОЙ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СЕТЯХ

В настоящее время наблюдается бурное развитие сетей и их использование в коммерческой деятельности при продаже различных товаров и услуг. Естественно, остро встает вопрос защиты информации от несанкционированного доступа (НСД) как недоброжелателей извне, так и самих сотрудников фирм. По мнению экспертов, чтобы парализовать жизненно важные точки созданной инфраструктуры, достаточно нанести удар всего по нескольким десяткам объектов. Уже сегодня, по заявлению некоторых иностранных экспертов, отключение компьютерных систем приведет к разорению 20% средних компаний и около 33% банков в течение нескольких часов, 48% компаний и 50% банков потерпят крах в течение нескольких суток.

Количество компьютерных преступлений в кредитно-финансовой сфере постоянно возрастает. Например, английские магазины фиксируют до 25% мошеннических платежных операций. При опросе 1 600 специалистов из 50 стран мира были получены следующие результаты:

– серверы, связанные с продажей продуктов или услуг через Интернет, подвергаются нападению почти на 10% чаще, чем серверы, не используемые для проведения финансовых сделок;

– 22% фирм, занимающихся продажами через Web-серверы, имели потери информации, и только 13% компаний, не продающих продукты через Интернет, столкнулись с этой же проблемой;

– 12% респондентов, имеющих электронные магазины, сообщили о краже данных и торговых секретов, и только 3 таких случая зафиксировано у компаний, не продающих продукты через систему Web.

Сумма потерь в результате различного рода мошенничества в сфере банковских услуг и финансовых операций составила:

– 1989 г. – 800 млн долл. США;

– 1992 г. – 1,2 млрд долл. США;

– 1993 г. – 1,78 млрд долл. США;

– 1997 г. – 100 млрд долл. США.

Эти показатели продолжают расти, но на самом деле эти цифры неточные. Реально они могут превышать приведенные данные на порядок. Так, например, профинансированные министерством обороны США испытания показали удивительные результаты. Специальные группы экспертов провели анализ защищенности 8 932 военных информационных систем. В 7 860 (88%) случаев проникновение в «святая святых» было успешным. Администраторы только 390 из этих систем обнаружили атаки, и только 19 сообщили о них. Другими словами, в 5% систем зафиксировали атаки, и только в 0,24% случаях от общего количества числа успешно атакованных систем (или 4,9% от числа зафиксировавших атаки) было заявлено об этом в соответствующие инстанции.

В зависимости от мотивов, целей и методов действия нарушителей безопасности информации можно разделить на следующие категории:

– искатели приключений;
– идейные хакеры;
– хакеры-профессионалы;
– ненадежные (неблагополучные) сотрудники.

К основным целям злоумышленника при внедрении в чужой компьютер можно отнести:

– получение необходимой информации в требуемом для конкурентной борьбы объеме и ассортименте;
– возможность внесения изменений в информационные потоки конкурента в соответствии со своими интересами;
– нанесение ущерба конкуренту путем уничтожения материала информационных ценностей.

Практика показала, что только в 20–30% НСД происходит с использованием удаленных атак за счет несовершенства Интернет-протоколов, что позволяет взломщикам осуществить анализ сетевого трафика сети, внедрить ложный объект сети и внедрить ложный маршрут. Остальные 70–80% нарушений осуществляются сотрудниками самих фирм или с их помощью.

К наиболее типовым удаленным атакам на информацию в сети из-за несовершенства Интернет-протоколов относятся:

– анализ трафика сети;
– внедрение ложного объекта сети;
– внедрение ложного маршрута.



Здесь также следует напомнить и о компьютерных вирусах, и в первую очередь о так называемых, «троянских конях», «враждебных апплетах Java» и «червях».

«Троянский конь», как видно из названия, представляет собой программу, которая имеет скрытную функцию, способную нанести вред компьютеру. «Троянский конь» обычного типа распространяется по электронной почте с целью скопировать пароль доступа компьютера, а затем пересылает украденные данные анонимному получателю.

«Враждебные апплеты Java» служат для захвата информации или наносят ущерб компьютерным пользователям, которые посещают Web-узлы конкурентов. Пользователь может стать жертвой такой программы, когда щелкает на ссылку, полученную им по электронной почте.

«Черви» используют такие компьютерные ресурсы, как память и сетевую полосу пропускания, из-за чего замедляется работа компьютеров и серверов. Кроме того, «черви» иногда удаляют данные и быстро распространяются по электронной почте.

Жизненный цикл компьютерных вирусов может включать следующие этапы:

– внедрение (инфицирование);
– инкубационный период;
– саморазмножение (репродуцирование);
– выполнение специальных функций;
– проявление.

Если компьютер работает под управлением ОС Windows, то «троянские кони» могут быть выявлены по наличию соответствующих записей в системном реестре. Например, «троянский конь» Donald Dick опознается по присутствию раздела HKLM\System\CurrentControlSet\Service\VxD\VMLDR (для операционных систем Windows 95 и 98) или HKLM\System\CurrentControlSet\Control\SessionManager (для ОС Windows NT), «троянский конь» BackOrifice может «оставить следы» в системном реестре HKLM\Softwere\ Microfoft\Windows\CurrentVersion\RunServices. Данный раздел системного реестра, а также разделы Run, RunOnce, RunServiceOnce и RunOnceEx очень часто используются «троянскими программами», автоматически загружающимися вместе с операционной системой. Например, «троянец» NetBus отлавливается по наличию ключа с названием загружаемого файла Patch.exe.

Еще одним способом обнаружения «троянских программ» является контроль файлов, поскольку большинство «троянцев» имеют заранее известные имена файлов и выявление их на компьютере можно расценивать как несанкционированную деятельность. Например, файл с именем Patch.exe – повод задуматься о присутствии на узле «троянца» NetBos, Digital, RootBeer, Krenx или Solid Gold.

Кроме описанных выше вариантов доступа к информации, существуют еще так называемые шпионские программные закладки. Программная закладка – это программа, скрытно внедренная в защищенную систему (или дописанный фрагмент пользовательской программы), позволяющая злоумышленнику путем модификации свойств системы защиты осуществлять несанкционированный доступ к ресурсам системы (в частности, к конфиденциальной информации). Если программа написана грамотно, то после ее внедрения в систему обнаружить ее стандартными средствами администрирования практически невозможно, она может функционировать неограниченно долгое время, и злоумышленник, внедривший закладку, имеет практически неограниченный доступ к системным ресурсам. С помощью этих программ можно осуществлять перехват вводимый паролей, переносить исходные данные из одной области оперативной или внешней памяти компьютера в другие, искажать информацию и т. п.

Для предотвращения или нейтрализации последствий информационных атак рекомендуется применять следующие меры:

– защита материально-технических объектов, составляющих физическую основу информационных ресурсов;

– обеспечение нормального и бесперебойного функционирования баз и банков данных;

– защита информации от НСД, ее искажения или уничтожения;

– сохранение качества информации (своевременности, точности, полноты и необходимой доступности).

Для этой цели следует использовать такие программы, как Firewall, Outpost, и в коммерческой деятельности eTrust for Ebusiness и др.

Как было сказано выше, в 70–80% случаях НСД осуществляется работниками данной фирмы. Побудительными мотивами таких сотрудников являются:

– реакция на выговор или замечание со стороны руководителя;

– недовольство тем, что фирма не оплатила сверхурочные часы работы;



– злой умысел в качестве, например, реванша с целью ослабления фирмы как конкурента какой-нибудь вновь создаваемой фирмы.

Недовольный руководителем служащий создает одну из самых больших угроз вычислительным системам коллективного пользования.

Для предотвращения НСД некоторые крупные фирмы предпочитают нанимать на работу хакеров и платят им за это большие деньги.

Коммерческую информацию можно подразделить на три уровня информация для служебного пользования (информация, которую может получить любой сотрудник фирмы), информация для среднего звена фирмы и информация для руководства фирмы.

Исходя из этого следует использовать и соответствующие пароли для получения конкретной информации, которые подразделяются: на пароли, установленные пользователем; пароли, генерируемые системой; случайные коды доступа, генерируемые системой; полуслова; ключевые слова; интерактивные последовательности типа «вопрос–ответ»; «строгие пароли».

Для защиты компьютерных сетей или отдельных компьютеров от НСД применяются три основных вида контроля доступа, основанные на владении физическим ключом, личностных характеристиках пользователя, обладании специфической информации.

Когда говорят о контроле доступа, основанном на владении физическим ключом, речь идет о предметах, принадлежащих пользователю: физическом ключе, магнитной карте, металлической пластинке причудливой формы, которую вставляют перед началом работы в щель распознавателя.

Для контроля доступа, основанного на личностных характеристиках пользователя, используются биометрические приборы, анализирующие специфические физические особенности пользователя (подпись, тембр голоса, отпечатки пальцев, рисунок линий на ладони или на сетчатке глаза и т. п.) и сравнивают их с теми, что находятся в памяти приборов.

Компьютерная защита этих двух видов может использоваться и для дистанционного управления доступом, хотя обычно к ней прибегают для ограничения доступа к компьютерному залу или отдельному кабинету – помещению, где находятся компьютеры.

Контроль доступа, основанный на обладании специфической информацией, наиболее распространен и характеризуется тем, что правом доступа обладают лишь те лица, которые способны проде-

монстрировать свое знание определенного секрета, обычно – пароля. Это самый простой и дешевый способ защиты любой компьютерной системы. Поскольку его использование не требует больших затрат времени, сил, а также памяти компьютера, то он применяется даже в тех компьютерах, которые вовсе не нуждаются в средствах защиты.

Кроме того, использование пароля создает у пользователя ощущение психологического комфорта. Этот способ защиты широко используется в системах, уже защищенных другими средствами – магнитными картами или иными программными методами типа шифрования, это в еще большей степени укрепляет защиту от несанкционированного доступа.

Пароли, как правило, рассматриваются в качестве ключей для входа в систему, но они используются и для других целей: блокирование записи на дисковод, в командах на шифрование данных, т. е. во всех случаях, когда требуется твердая уверенность, что соответствующие действия будут производиться только законными владельцами или пользователями программного обеспечения.

Чтобы пароль оказался действительно надежным, он должен отвечать следующим требованиям:

– быть определенной длины;
– включать в себя как прописные, так и строчные буквы;
– включать в себя одну и более цифр;
– содержать один нецифровой и один неалфавитный символ.

Рекомендуется соблюдать одно или несколько из этих правил.

УДК 50.37.23

© И. В. Поночевная, З. Н. Аргеровская

Санкт-Петербургский государственный инженерно-экономический университет

## КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Как организована защита компьютерной сети? Опасности грозят со всех сторон, они настолько многочисленны, что кажется невозможным найти согласованное решение.



При рассмотрении вопроса о защите браузеров, приложений, баз данных, корпоративных серверов, хостов, брандмауэров, шлюзов и маршрутизаторов в интрасети выявляется множество возможностей для взлома, чтобы проникнуть в сеть, подслушать, украсть информацию, заразить сеть вирусами или полностью ее разрушить. Никогда невозможно полностью защититься от кражи информации или злоупотреблений со стороны собственных сотрудников, которые могут перемещаться по сети, не вызывая подозрений.

Нарушения защиты сети происходят настолько часто, что способны вывести из состояния душевного равновесия даже наиболее благодушно настроенных администраторов сетей и систем.

Взять в свои руки защиту сетевых ресурсов, безусловно, дело непростое, а быстрое изменение технологий и стандартов еще больше его усложняет. Концепции защиты браузера, Web-узла и брандмауэра еще не проработаны; администраторы сетей совсем недавно начали систематизировать свою деятельность, связанную с этой проблемой.

Можно решать вопросы, связанные с защитой сети, по мере возникновения кризисов или принимать рациональные упреждающие систематические меры. Реализация систематической защиты сети в принципе не отличается от традиционной защиты сетей и систем. При этом большинство вопросов группируются по трем категориям: защита клиента, защита сервера и защита шлюза.

Браузеры – основные, но не единственные, пункты защиты клиента в компьютерной сети. Они могут оказаться не более защищенными, чем операционные системы и рабочие станции, на которых запускаются эти браузеры. Если исходить из традиционных критериев, предъявляемых к информационным системам, то современные Web-браузеры – очень уязвимые клиентские приложения.

Среди самых уязвимых мест современных коммерческих браузеров – отсутствие защиты паролем, неограниченный доступ к локальным ресурсам компьютера и возможность раскрытия критически важных данных при помощи кнопок «вперед/назад», закладок и выделенных цветом ссылок.

Опытные пользователи «обходят» уязвимые места, реализуя клиентские приложения, которые имеют функции защиты.

Многие считают, что браузеры и рабочие станции, на которых они установлены, имеют вполне достаточную защиту, а Интранет- и Интернет-соединения доверия не внушают.

Чтобы снять этот вопрос, в большинстве коммерческих браузеров была реализована поддержка версий протокола шифрования Secure Sockets Layer (SSL) 2.0 и 3.0, предназначенных для защиты трансакций, которые осуществляются в соответствии с HTTP, FTP и другими протоколами Интернета. SSL использует шифрование с открытым ключом для обмена в одном сеансе 40- или 128-разрядным ключом между браузером и Web-сервером. Ключ сеанса применяется для шифрования как запроса, так и ответа при интерактивной трансакции; личные ключи пользователя и сервера сохраняются в секрете.

Аутентификация и возможности шифрования в SSL довольно выразительны, но ненадежны. Как показали исследования, современные вычислительные средства позволяют преодолеть защиту поддерживающих SSL браузеров, таких как Netscape Navigator.

Тем не менее, не все администраторы сети обеспокоены уровнем безопасности SSL. Защита сети во многом зависит от того, можем ли мы доверять программным компонентам (управляющим элементам, подключаемым модулям и другим исполняемым компонентам), которые браузеры постоянно загружают и устанавливают повсюду.

Криптография как средство защиты (закрытия) информации является в настоящее время актуальной в системе подготовки специалистов инженерно-экономических специальностей, формирующей общую информационную культуру навыков работы с информацией, составляющей коммерческую и служебную тайну, а также теоретические и практические знания по обеспечению информационной безопасности в компьютерных системах.

Современные криптографические системы позволяют шифровать сообщения так, что на их раскрытие могут понадобиться десятки, сотни лет непрерывной работы.

Основные направления использования криптографических методов – это передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

В настоящее время используются различные компьютерные криптоалгоритмы и программы для шифрования данных, наиболее известные из них DES, RSA, PGP, ГОСТ 28147-89. Современные криптографические системы обеспечивают высокую надежность зашифрованных данных за счет поддержания режима секретности криптографического ключа.



Кодирование и шифрование – основные методы криптографической защиты.

УДК 50.37.23

© С. А. Соколовская

Санкт-Петербургский государственный инженерно-экономический университет

## СИСТЕМЫ БЕЗОПАСНОСТИ SQL SERVER 2000

В современных условиях информация имеет огромное значение, поэтому принятие мер для предотвращения несанкционированного доступа, предотвращения потери или повреждения информации становится неотъемлемой частью благополучного существования любой компании. Выход информации за пределы компании может принести большие убытки. По данным статистики, в США 80% компаний, потерявших информацию, прекращали свою деятельность в течение одного года.

Активное использование SQL Server 2000 в электронной коммерции и Web предполагает рост требований к системе безопасности. Понимая это, разработчики Microsoft приложили немало усилий для повышения надежности защиты информации.

SQL SERVER 2000 в своем арсенале имеет разнообразные средства обеспечения защиты данных:

– средства обеспечения безопасности доступа к SQL Server (идентификация пользователя, аутентификация, авторизация);

– система безопасности на основе ролей, определяющих права доступа к серверу, базе данных и приложениям;

– средства передачи информации.

Существенно усилены средства аудита – появилась возможность отслеживания 18 типов классов, связанных с безопасностью, и дополнительных подклассов. Теперь администратор может отслеживать не только успешные или неудачные попытки установления соединения с SQL Server, но и более детально – доступ к объектам, их создание и удаление, изменение прав доступа и т. д. В SQL Server 7.0 отслеживание этих событий происходило лишь при выполнении

трассировки с помощью утилиты SQL Server Profiler или соответствующих хранимых процедур команд, выполняемых в пользовательских сессиях.

Шифрование – это метод, используемый SQL Server для изменения данных до нечитаемой формы. Использование шифрования гарантирует, что ценная информация при передаче по сети не будет потеряна.

Шифрование в SQL Server 2000 поддерживается и на уровне сетевого трафика, и на уровне файлов баз данных, в отличие от SQL Server 7.0, где существовала возможность непосредственного просмотра файлов базы данных и беспрепятственного использования нелегально скопированных баз данных. Шифрование же на уровне файлов дополнительно повышает безопасность информации. Для обеспечения безопасности сетевых соединений служат протоколы SSL и Kerberos.

УДК 50.37.23

**© А. И. Соловьев**

Санкт-Петербургский государственный
инженерно-экономический университет

## СОВРЕМЕННЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Развитие информационных технологий привело к возникновению новых форм экономической деятельности, таких как электронная торговля и электронная коммерция или e-Commerce. Электронная коммерция – это заключение и исполнение сделок в электронной форме, что влечет за собой необходимость решения вопросов ее правового, финансового, организационного, информационного и технического обеспечения. Тогда как электронная торговля включает в себя заказ товаров и их оплату с использованием сети Интернет, что является частью электронной коммерции.

В настоящее время получили развитие две модели глобальной электронной коммерции: B2B – business-to-business – торговые отношения между предприятиями и B2C – business-to-customer – торговые отношения между предприятием и покупателем.

Объем мирового оборота электронной коммерции через Интернет в 2003 г., по прогнозам компании «Forrester Tech.», может составить от 1,8 до 3,2 трлн долл. Столь широкий диапазон прогноза определяется проблемой обеспечения экономической безопасности электронной коммерции. Если уровень безопасности сохранится в соответствии с сегодняшним, то мировой оборот электронной коммерции может оказаться еще меньше. Отсюда следует, что именно низкая экономическая защищенность системы электронной коммерции является сдерживающим фактором развития электронного бизнеса.

Решение проблемы обеспечения экономической безопасности электронной коммерции в первую очередь связана с решением вопросов защиты информационных технологий, применяемых в электронной коммерции, т. е. с обеспечением информационной безопасности.

Электронная коммерция объединяет множество различных функций. В ней используются новые технологии для организации контакта покупателей и продавцов, методов представления, обсуждения и формирования заказа, определения условий сделки, порядка продажи товаров и услуг, а также для процесса осуществления платежей.

В настоящее время существует достаточно большое количество программных решений для организации электронного бизнеса. В России развитие электронной коммерции сдерживается:

– недостаточно развитой инфокоммуникационной инфраструктурой;

– высокой уязвимостью для злоумышленников;

– нарастающей степенью конкурентной борьбы.

Как видно, все перечисленные препятствия относятся к сфере информационной безопасности.

К сожалению, руководители предприятий электронной коммерции в должной степени осознают серьезность информационных угроз и важность организации защиты своих ресурсов только после того, как подвергнутся информационным атакам.

Рассмотрим некоторые варианты обеспечения экономической защищенности компаний электронной коммерции. Причем это не сводится только к обеспечению доверия участников к процессу организации транзакций. Важно на каждом этапе электронного бизнеса обеспечивать их безопасность.

Процесс электронной коммерции в укрупненном виде включает семь этапов:

– выбор продукта или услуги на сервере компании и оформление заказа;

– внесение заказа в базу данных магазина;

– проверка доступности заказанного продукта через центральную базу данных;

– при отсутствии продукта и невозможности его своевременной поставки осуществляются уведомление об этом и коррекция заказа;

– при наличии продукта заказчик подтверждает заказ, и заказ размещается в базе данных на выполнение;

– оплата клиентом заказа в режиме on-line;

– поставка заказанного товара клиенту.

Угрозы, подстерегающие компанию, ведущую электронную коммерцию, на каждом этапе.

1. Подмена Web-страницы сервера электронного магазина, т. е. переадресация запросов на другой сервер, что делает доступными сведения о клиенте, особенно о его кредитных картах, сторонним лицам.

2. Создание ложных заказов и разнообразные формы мошенничества со стороны сотрудников электронного магазина, например, манипуляции с базами данных. Статистика свидетельствует о том, что больше половины компьютерных инцидентов связаны с собственными сотрудниками.

3. Перехват данных, передаваемых в сетях электронной коммерции.

4. Проникновение во внутреннюю сеть компании и компроментация компонентов электронного магазина.

5. Реализация атак типа «отказ в обслуживании» и нарушение функционирования или вывода из строя узла электронной коммерции.

В результате реализации таких угроз компания теряет доверие клиентов, теряет деньги от потенциальных и/или несовершенных сделок, нарушается деятельность электронного магазина, затрачивает время, деньги и человеческие ресурсы на восстановление функционирования.

Следует отметить, что угрозы связанные с перехватом передаваемой в Интернете информации, присущи не только электронной коммерции. Для систем электронной коммерции особое значение представляет то, что там обращаются сведения, имеющие важное



экономическое значение: номера кредитных карт, номера счетов, содержание договоров и т. п. Она не должна быть доступна третьим лицам.

В 2000 г. зафиксирован массовый выход из строя «отказ в обслуживании» популярных и ведущих серверов электронного бизнеса за счет многократного увеличения количества запросов на обслуживание. Поток запросов на сервер Buy превысили средние показатели в 24 раза, а предельные в 8 раз. По разным оценкам, нанесенный ущерб достиг 1,5 млрд долл.

Решением проблемы информационной безопасности электронного бизнеса занимается независимый консорциум – Internet Security Task Force (ISTF) – общественная организация, состоящая из представителей и экспертов компаний-поставщиков средств информационной безопасности, электронных бизнесов и провайдеров Интернет-услуг.

Консорциум ISTF выделяет 12 областей информационной безопасности, на которых в первую очередь должно быть сосредоточено внимание организаторов электронного бизнеса:

– механизм объективного подтверждения идентифицирующей информации;

– право на персональную частную информацию;

– определение событий безопасности;

– защита корпоративного периметра;

– определение атак;

– контроль за потенциально опасным содержимым;

– контроль доступа;

– администрирование;

– реакция на события.

От защиты перечисленных областей зависит непрерывность бизнеса со всеми вытекающими отсюда экономическими последствиями. Безопасность более не является дополнительным свойством: даже в 97% случаях надежность системы означает, что за год для бизнеса будут потеряны 293 ч.

Безусловно, обеспечением информационной безопасности должны заниматься специалисты в данной области, но руководители предприятий, отвечающие за экономическую безопасность, должны постоянно держать данные вопросы в поле своего зрения. Для них

ниже приведены основные подходы к организации комплексной системы информационной безопасности на основе следующих функциональных компонентов:

– коммуникационные протоколы;

– средства криптографии;

– механизмы авторизации и аутентификации;

– средства контроля доступа к рабочим местам и из сетей общего пользования;

– антивирусные комплексы;

– программы обнаружения атак и аудита;

– средства централизованного управления контролем доступа пользователей, а также безопасного обмена пакетами данных и сообщений любых приложений по открытым сетям.

Решение проблемы информационной безопасности электронной коммерции является наиболее важным для обеспечения экономической безопасности электронного бизнеса.

УДК 50.37.23

**© М. И. Сотемская**

Санкт-Петербургский государственный
инженерно-экономический университет

## АНАЛИЗ И РАСЧЕТ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ[1]

Давно известно, что информация может быть настоящим сокровищем. Тот, кто владеет информацией, неизбежно затрачивает много усилий на обладание ею и охрану. Владелец информации создает надежные системы защиты своей собственности, которые в свою очередь имеют смысл с точки зрения результата относительно затрат. Таким образом, затраты и безопасность необходимо рассматривать и анализировать совместно, соизмеряя их с ресурсами и рисками.

Одним из наиболее применяемых на практике вариантов анализа, дающим первоначальную оценку состояния информационной

[1] Данная статья поддержана грантом Министерства образования РФ по фундаментальным исследованиям в области гуманитарных наук ГО2-4.1-15.



системы (ИС) предприятия по средствам защиты информации, является аудит системы безопасности информационных ресурсов на предприятии.

Аудит безопасности ИС представляет собой независимую экспертизу состояния различных областей системы организации. Целями проведения аудита безопасности являются:

– анализ рисков, связанных с угрозами безопасности ресурсов ИС;

– оценка текущего уровня защищенности ИС;

– локализация узких мест в системе защиты ИС;

– оценка соответствия ИС существующим стандартам в области информационной безопасности;

– выработка мероприятий по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Подходы к проведению аудита безопасности базируются на анализе рисков и опираются на использование стандартов информационной безопасности.

Анализ рисков – то, с чего должно начинаться построение системы информационной безопасности предприятия. Это ряд мероприятий по обследованию безопасности ИС на предмет того, «что от кого» надо защищать, а также в какой степени и какие ресурсы нуждаются в защите.

Риск определяется величиной ущерба информационной системе в случае осуществления угрозы безопасности.

Анализ рисков заключается в выявлении риска, оценке его величины в качественном и количественном эквиваленте.

Ресурсы ИС можно разделить на следующие категории:

– информационные ресурсы;

– программное обеспечение (ПО);

– технические средства;

– людские ресурсы.

При делении ресурсов на классы и подклассы можно проследить зависимости между видом ресурса и функциональностью ИС. Необходимо выделять виды ресурсов, существенных с точки зрения обеспечения безопасности. Величина причиненного ущерба в случае нарушения конфиденциальности или целостности определяет важ-

ность (стоимость) данного вида ресурса. Чаще всего рассматривают следующие виды ущерба:

– раскрытие, изменение, удаление данных или их последующая недоступность;

– повреждение, разрушение аппаратуры;

– нарушение целостности ПО.

Ущерб может быть расценен в результате осуществления следующих видов угроз безопасности:

– локальные и удаленные атаки на ресурсы ИС;

– стихийные бедствия;

– ошибочные или умышленные действия персонала;

– сбои в работе ИС, вызванные ошибками в ПО или неисправностями аппаратуры.

Величина риска определяется на основе стоимости ресурса, вероятности осуществления угрозы и величины уязвимости:

$$\text{Риск} = \frac{\text{Стоимость ресурса} \times \text{Вероятность угрозы}}{\text{Величина уязвимости}},$$

где под величиной уязвимости будем понимать свойства ИС, дающие наибольшую вероятность «успешного» осуществления угроз безопасности.

Задача управления рисками состоит в выборе обоснованного оптимального набора контрмер, позволяющих исключить или максимально снизить уровни рисков. Стоимость контрмер должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть обратно пропорциональна вероятности причинения ущерба.

В зависимости от размеров организации, ее доходов и положения на рынке, руководство определяет последствия потери ресурсов (в стоимостном выражении) методом экспертных оценок.

Анализ рисков позволяет смоделировать набор мероприятий по защите информации на предприятии и наиболее точно определить объем затрат на систему защиты информации на предприятии исходя из доходов предприятия, сферы деятельности и целесообразности тех или иных мер.



УДК 50.37.23

© М. И. Сотемская, К. Ю. Тяпкина

Санкт-Петербургский государственный инженерно-экономический университет

# ОБЗОР ОСНОВНЫХ ТЕХНОЛОГИЙ ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ[1]

Любая информация содержит определенное смысловое содержание и прикреплена к конкретному носителю. Для компьютерной информации таким носителем может быть файл, поле базы данных, данные любого из программных приложений. Очевидно, что носителем информации также являются каталог или жесткий диск персонального компьютера или сервера, на котором хранится файл (поле БД и т. п.). Также следует учитывать, что требует защиты не только сама информация, но и среда ее обработки, т. е. программное обеспечение.

Защита информации состоит из трех компонентов:

– защита смыслового содержания информации, т. е. сохранение конфиденциальности и целостности информации;

– защита носителя от несанкционированного доступа к нему;

– защита информации от сбоев в сети электропитания, пожаров.

В современных комплексных системах информационной безопасности применяются самые передовые технологии защиты информации. К ним относятся: межсетевое экранирование, технология виртуальных защищенных сетей (VPN-технология), антивирусные программы, активный аудит и мониторинг сети, защита от несанкционированного доступа, технология BioLinkTM, криптографические методы, eSafe.

Межсетевые экраны – программные или программно-аппаратные средства, предназначенные для создания защищенного периметра ЛВС организации с контролируемыми точками входа, защищенного подключения корпоративной сети к сетям общего пользования, Интернету; разграничения доступа к ресурсам внутри корпоративной сети; а также для обеспечения контроля информационных потоков

[1] Данная статья поддержана грантом Министерства образования РФ по фундаментальным исследованиям в области гуманитарных наук ГО2-4.1-15.

между различными сегментами корпоративной сети и внешними сетями. К таким средствам относится, в частности, один из ведущих продуктов фирмы «Информзащита», который называется аппаратно-программный комплекс шифрования (АПКШ) «Континент».

Использование VPN-технологии исключает возможность перехвата информации, подключения незарегистрированного компьютера, изменения информации и любые сетевые атаки. Данные, подлежащие передаче, шифруются на «выходе» из одной сети и расшифровываются на «входе» другой сети. Таким образом, возможно организовать защиту информации на любом уровне: защита трафика (всей информации, передаваемой по каналу связи), между сервером и пользователем, между клиентами.

Антивирусные программы наиболее эффективны в борьбе с компьютерными вирусами. Однако не существует программы, гарантирующей 100%-ю защиту от вирусов. Качество антивирусных программ определяется надежностью и удобством работы, качеством обнаружения вирусов всех распространенных типов, существованием версии антивируса под все популярные платформы, сканированием по запросу и «на лету», скоростью работы и другими параметрами.

Еще одним решением поставленной проблемы является такая модель работы средств защиты, при которой защита реализовывалась бы в реальном режиме времени, настройки средств защиты адаптировались бы к изменяющимся условиям инфраструктуры, безопасность осуществлялась бы не только на этапе атаки, но и на этапе подготовки к атаке, а также на этапе завершения атаки. Подход, на котором основано решение данной проблемы, получил название технологии активного или адаптивного управления безопасностью, или технологии активного аудита. Использование модели адаптивной безопасности сети позволяет контролировать практически все угрозы и своевременно реагировать на них высокоэффективным способом, позволяющим не только устранить уязвимости, которые могут привести к реализации угрозы, но и проанализировать условия, приводящие к появлению уязвимостей. Эта модель также позволяет повысить осведомленность администратора безопасности о событиях безопасности в сети.

Для защиты от несанкционированного доступа (НСД) к ресурсам ПК и локальной вычислительной сети, разграничения прав незарегистрированных пользователей по доступу к ресурсам ПК, автоматизированного контроля и протоколирования событий по доступу к компьютеру, чтения информации с экрана монитора, жестких и гибких магнитных дисков на серверы и ключевые рабочие станции устанавливается программно-аппаратный комплекс защиты от НСД. Защита ключевых рабочих станций достигается применением средств защиты информации типа «электронный замок», защита сетевых соединений – применением усиленной аутентификации рабочих станций и серверов, основанной на технологиях цифровой подписи, шифрования и инкапсуляции IP-пакетов.



Криптографические методы являются неотъемлемой частью многих технологий защиты информации. В частности, построение системы электронного документооборота, усиленная аутентификация пользователей в сети основаны на применении криптографической технологии – электронная цифровая подпись. Задачи защиты электронных документов при их передаче по открытым каналам связи, сетевого и межсетевого трафика при организации виртуальных частных сетей, а также защита информации на жестком диске компьютера решаются путем применения шифрования.

e-Safe – комплексная защита при работе в Интернете. Интернет – среда развития бизнеса, однако его применение связано с возникновением целого ряда угроз, защита от которых требует комплексного подхода. Технология e-Safe обеспечивает безопасность бизнеса, информации, сети и предлагает комплексные решения для защиты корпоративных сетей на уровне Интернет-шлюзов (e-Safe Gateway), почтовых серверов SMTP, серверов групповой работы MS Exchange/Lotus Notes (eSafe Mail), корпоративных ресурсов для серверов NT/2000/NetWare (e-Safe Enterprise). Основные преимущества технологии e-Safe – централизованное управление безопасностью, комплексный аудит информации и контроль всех рабочих станций из одной точки, сканирование, эвристический анализ, отслеживание и блокирование недопустимого и/или контрпродуктивного контента, опасных вложений, враждебных кодов, «традиционных» и новых вирусов, «троянов» и «вандалов», возможность интеграции с другими средствами защиты, уже используемыми в компании (межсетевыми экранами, антивирусами и т. д.).

Характерной чертой современных корпоративных систем является наличие сложной гетерогенной структуры, базирующейся на взаимодействии неоднородных программно-аппаратных компонент,

и высокая стоимость коммерческой информации, обрабатываемой в них. Данные факторы значительно усложняют задачу построения надежной и эффективной системы защиты информации на предприятии. В связи с этим усиливается необходимость комплексного подхода к построению системы информационной безопасности с использованием различных методов и технологий защиты в зависимости от каждого объекта системы и его свойств.

УДК 50.37.23

© Е. В. Стельмашонок

Санкт-Петербургский государственный инженерно-экономический университет

## ОПТИМИЗАЦИЯ ВЫБОРА СХЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ТЕОРЕТИКО-ИГРОВОЙ МОДЕЛИ[1]

Перед фирмами, предприятиями, заинтересованными в защите информации, стоит сложная задача выбора средств защиты, требующих достаточно значительных материальных затрат. Для обоснованного выбора средств защиты необходимо оценить экономическую целесообразность защиты информации.

Для оптимального формирования набора средств защиты информации можно использовать метод теории игр, который позволяет решать поставленную задачу в условиях неопределенной информации о действиях «злоумышленника». Для этого модель задачи строится как модель проектанта (второго игрока) против «природы» (первого игрока – фиктивного игрока, стратегии которого нам неизвестны). Можно рассмотреть несколько критериев проведения игр такого типа. В данном случае выбирается критерий Вальда (принцип минимакса), соответствующий пессимистической теории ожидания худшего.

Стратегии проектанта (второго игрока): выбор $x_{jk}$ – средств защиты $j$-го типа от угроз $k$-го вида при ограничениях (1) и (2):

$$x_{jk} = 0, 1, 2, \ldots, N_j, \tag{1}$$

[1] Данная статья поддержана грантом Министерства образования РФ по фундаментальным исследованиям в области гуманитарных наук ГО2-4.1-15.



где $N_j$ – максимально возможное количество средств защиты $j$-го типа.

Ограничение (1) говорит о целочисленности значений $x_{jk}$.

$$\sum_{k=1}^{n} x_{jk} \le N_j (j = 1, 2, \ldots, m), \tag{2}$$

где $m$ – количество типов средств защиты;

$n$ – число рассматриваемых угроз.

Стратегии «природы» (первого игрока): выбор $y_{jk}$ (руб.) – причиняемого «злоумышленником» ущерба, возможного в результате неиспользования средства защиты $j$-го типа от угрозы $k$-го вида при ограничениях (3), (4):

$$\sum_{k=1}^{n} y_{jk} \le \sum_{k=1}^{n} x_{jk}, \tag{3}$$

$$a_k \le \sum_{j=1}^{m} y_{jk} \le b_k, \tag{4}$$

где $a_k$ – минимально возможный ущерб, наносимый «злоумышленником» при реализации угрозы $k$-го вида;

$b_k$ – максимально возможный ущерб, наносимый «злоумышленником» при реализации угрозы $k$-го вида.

Оптимальная стратегия проектанта будет определяться из (5):

$$S = S_h + S_j, \tag{5}$$

где $S_h$ – сумма ущерба, наносимого «злоумышленником»;

$S_j$ – затраты, связанные с использованием средств защиты.

Модель формирования оптимального набора средств защиты информации может быть описана с помощью игровой задачи, связанной с распределением двумя игроками ресурсов нескольких типов между несколькими участками.

Методы решения такой игровой задачи различны. Одним из них является метод, который рассматривает такую задачу как сумму матричных игр специального вида и сводит эту задачу к задаче линейного программирования. Указанный метод является такой организацией модифицированного алгоритма симплекс-метода с базисом переменного размера, при котором на каждом шаге нужно хранить и об-

рабатывать только «существенную» часть обратной матрицы базиса и линейных массивов.

При анализе систем защиты информации предполагается построение моделей затрат, связанных с созданием и использованием систем защиты информации.

Для решения задачи синтеза защищенной информационной системы будет приведена содержательная и формализованная постановка задачи синтеза защищенной информационной системы. Оптимальный вариант защиты информации предполагается получить на основе использования метода решения сумм матричных игр.

Этот метод строится на основе метода решения сумм матричных игр. Задача оптимизации выбора схемы защиты информации рассматривается как сумма $G$ матричных игр

$$G_{11}, \ldots, G_{m1}, \ldots, G_{1n}, \ldots, G_{mn},$$

в которой множеством $I$ чистых стратегий первого игрока является некоторое множество $(m \times n)$-мерных векторов

$$i = (i_{11}, \ldots, i_{1n}, \ldots, i_{m1}, \ldots, i_{mn}),$$

множеством $J$ чистых стратегий второго игрока является множество $(m \times n)$-мерных векторов

$$j = (j_{11}, \ldots, j_{1n}, \ldots, j_{m1}, \ldots, j_{mn}).$$

Матрицей выигрышей игры $G$ является матрица $M[Y, J]$, в которой

$$M[i, j] = \sum_{l=1}^{m} \sum_{k=1}^{n} H_{lk}[i_{lk}, j_{lk}]. \qquad (6)$$

Здесь $H_{lk}[A_{lk}, N_{lk}]$ – матрица игры $G_{lk}$, через $A_{lk}$ обозначим множество чистых стратегий первого игрока, а через $N_{lk}$ – множество чистых стратегий второго игрока в игре $G_{lk}$, причем $i_{lk} \in A_{lk}, j_{lk} \in N_{lk}$.

Каждой чистой стратегии первого игрока поставим в соответствии вектор $x_i$, компонентами которого являются нули и единицы.

Компоненты вектора $x_i$ объединены в $mn$ групп, причем в группе $l_k$, состоящей из $A_l$ компонент, единица стоит на $i_{lk}$-ом месте, а на всех остальных местах стоят нули.

Множество всех таких строк $x_i$ $(i \in I)$ объединено в матрицу $X$.

Аналогично каждой чистой стратегии второго игрока поставим в соответствии вектор $y_j$, компонентами которого являются нули и



единицы. Компоненты вектора объединим в $mn$ групп, причем, в группе $l_k$, состоящей из $N_l + 1$ компонент, единица стоит на $j_{lk}$-м месте, а на всех остальных местах стоят нули.

Множество всех векторов-столбцов $y_j (j \in J)$ объединены в матрицу $Y$. Введем в рассмотрение также блочно-диагональную матрицу $H$, составленную из блоков

$$H_{lk} (l = 1, 2, \ldots, m;\ k = 1, 2, \ldots, n).$$

Имеет место следующее представление:

$$M = XHY. \qquad (7)$$

Показывается, что ранг матрицы выигрышей соответствующей игры является относительно небольшим в сравнении с размерами самой матрицы, а значит у игроков существуют оптимальные смешенные стратегии, содержащие не более, чем $n\sum_{l=1}^{m} N_l + 1$ ненулевых компонент.

Если значение игры положительно, то исходная игра сводится к следующей задаче линейного программирования:

$$\max \sum_{j \in J} \omega_j, \qquad (8)$$

$$M_\omega \le 1, \qquad (9)$$

$$\omega \ge 0. \qquad (10)$$

Если $\{\omega_j^0\}$ – решение задачи (8)–(10), то оптимальная стратегия $\{\overline{\omega}_j\}$ второго игрока вычисляется по формуле

$$\overline{\omega}_j = \frac{\omega_j^0}{\sum_{j \in J} \omega_j^0} \ (j \in J), \qquad (11)$$

и если $\{u_i^0\}$ – решение задачи, двойственной к задаче (10)–(12), то оптимальная стратегия $\{\overline{u}_i\}$ первого игрока вычисляется по формуле

$$\overline{u}_i = \frac{u_i^0}{\sum_{i \in I} u_i^0} \ (i \in I). \qquad (12)$$

Вводятся переменные $v[l]$, дополняющие условия (9) до равенства

$$M \cdot \omega + E \cdot v = 1. \qquad (13)$$

где 1 – вектор, составленный из единиц.

Затем метод решения сумм матричных игр конкретизируется именно с учетом специфики игровых задач распределения ресурсов (специального задания множеств чистых стратегий игроков).

УДК 50.37.23

© В. В. Шлёнов

Санкт-Петербургский государственный
инженерно-экономический университет

## СТРАТЕГИИ И ТРЕБОВАНИЯ К КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ[1]

Развитие информационных технологий немыслимо без повышенного внимания предприятий к корпоративной информационной безопасности. Причиной тому является существование угроз безопасности для предприятия.

1. Обычные угрозы:
– природные катастрофы;
– технические отказы;
– вандализм.
2. Халатность персонала:
– недостаточное образование;
– отсутствие осторожности;
– отсутствие контроля мер безопасности.
3. Намеренные ошибки:
– некомпетентное использование данных;
– действия злоумышленников.

Статистика распределения наиболее крупных нарушений безопасности по видам атак на компьютерные системы предприятий США в 2003 г. (в процентах) показана на рис. 1 [1].

[1] Данная статья поддержана грантом Министерства образования РФ по фундаментальным исследованиям в области гуманитарных наук ГО2-4.1-15.



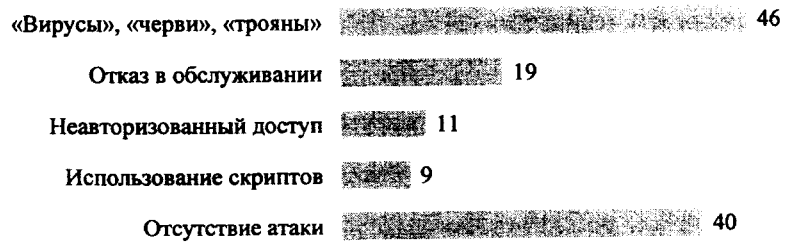



Рис. 1. Распределение наиболее крупных нарушений безопасности по видам атак

Распределение ущерба от нарушения компьютерной безопасности американских фирм в 2003 г. (в процентах) показано на рис. 2 [1].

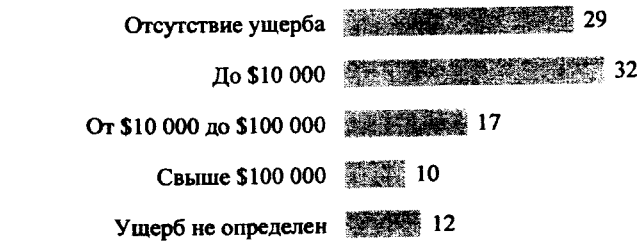



Рис. 2. Распределение ущерба от нарушений компьютерной безопасности по видам атак

Наиболее распространенные методы атак на компьютерные информационные системы предприятий Германии в 2002 г. (в процентах) приведены на рис. 3 [2].

Среди причин, которые сдерживают эффективность защиты корпоративных информационных систем в США, необходимо назвать следующие (в процентах указано наличие соответствующего фактора для группы обследуемых предприятий):

– растущее многообразие и изощренность атак (49%);
– недостаток времени (37%);
– ограниченность бюджета (45%);
– недостаток средств на изучение проблемы и обучение персонала (37%);
– высокие темпы изменений (28%);

– сложность технологий (24%);
– отсутствие комплексных продуктов защиты (27%);
– отсутствие стратегии информационной безопасности (22%);
– недостаточная квалификация персонала (31%).

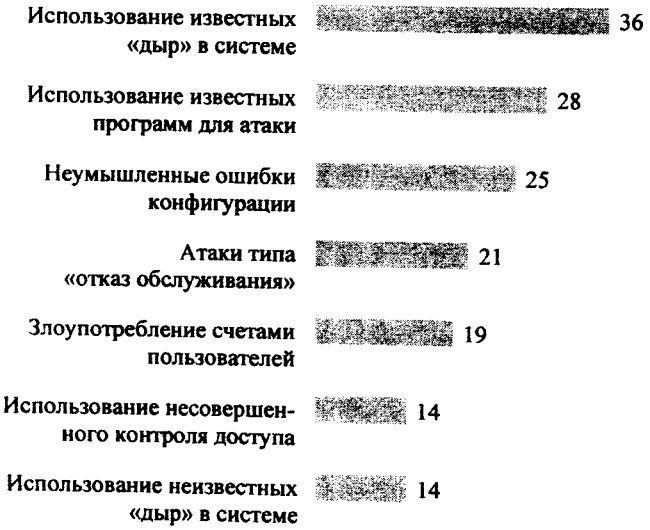



Рис. 3. Методы атак на компьютерные информационные системы

Финансовые потери из-за нарушения компьютерной безопасности включают в себя следующие ущербы:

– прямой ущерб:
  затраты на восстановление, ремонт и пусконаладочные работы;
  ущерб из-за потери секретности и целостности данных;
– косвенный ущерб, в том числе штрафы из-за нарушения сроков поставок;
– стратегический ущерб (потеря имиджа);
– специфический для предприятия ущерб:
  затраты из-за простоя производства;
  ущерб из-за простоя Интернет-магазина;
  ущерб из-за утечки клиентских данных к конкурентам;
  ущерб из-за кражи личных персональных данных.



Анализ вышеприведенных данных позволяет сделать следующие выводы.

1. Растет число и сложность нарушений компьютерной безопасности.

2. Несмотря на появление новых средств межсетевой и антивирусной защиты, вирусы, «черви» и «троянские кони» остаются угрозой номер один.

3. Растут финансовые потери в расчете на единичное нарушение компьютерной безопасности.

4. Главными факторами, сдерживающими эффективное внедрение средств защиты, являются сложность угроз, время, персонал и бюджет.

5. Служба информационной безопасности предприятия, как правило, отсутствует. Лишь немногие фирмы имеют сотрудника нижнего уровня иерархии, занимающегося исключительно вопросами информационной безопасности.

6. Информационная безопасность предприятия, как правило, остается вне поля зрения высшего руководства.

Предлагаемыми мерами повышения уровня информационной безопасности являются:

– разработка стратегических мероприятий безопасности:
  улучшение сетевой безопасности;
  защита от несанкционированного доступа;
  развитие архитектуры безопасности;
  развитие стратегий информационной защиты;
  гарантия обязательств на ведущем уровне;
– разработка тактических мероприятий безопасности:
  защита от вирусов и прочих враждебных кодов;
  улучшение защиты операционной системы;
  установка межсетевых экранов;
  ужесточение контроля доступа;
  улучшение защиты удаленного доступа;
  улучшение защиты приложений;
  аудит пользователей;
  улучшение защиты Web-браузеров.
– разработка требований к информационной безопасности:
  достижение стратегических целей и гарантий защиты данных [3];

создание менеджмента корпоративной информационной безопасности;
интеграция информационной безопасности в стратегию и бизнес-процессы предприятия.

**Литература**


1. www.informationweek.de/index.php3?/studien/studien.htm
2. www.informationweek.de/index.php3?/studien/studien.htm
3. *Шлёнов В. В.* Технологии защиты данных в Интернет // Современные информационные технологии в экономике и образовании: Сб. науч. тр. СПб.: СПбГИЭУ, 2001.


# Раздел II

# ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 330.190.2

**© И. Н. Анисимова**

Санкт-Петербургский государственный инженерно-экономический университет

## ОБРАБОТКА РЫНОЧНЫХ ДАННЫХ В ЗАДАЧАХ ИНДИВИДУАЛЬНОЙ ОЦЕНКИ НЕДВИЖИМОСТИ

Перспективным развитием оценочной теории и практики является применение регрессионных моделей и методов при решении задач индивидуальной оценки собственности в рамках сравнительного подхода. Сравнительный подход в оценочной деятельности основан на расчете стоимости объекта оценки исходя из сравнения его характеристик с характеристиками и известными ценами недавних продаж его аналогов на открытом конкурентном рынке данного вида имущества.

Сравнительный подход эффективен в случае существования развитого активного рынка сопоставимых объектов собственности. Данный подход неприменим для оценки уникальных объектов. Если сделок было мало и моменты их совершения разделяет длительный период; если рынок находится в аномальном состоянии, на нем происходят быстрые изменения, то действенность сравнительного подхода снижается. В настоящее время можно констатировать существование в крупных российских городах, в том числе и в Санкт-Петербурге, сформировавшегося конкурентного открытого рынка различных объектов движимого и недвижимого имущества (за исключением земельных участков), что позволяет в большинстве случаев практической оценки использовать приемы и методы сравнительного подхода.

Регрессионные методы в рамках такого подхода позволяют восстановить вид статистической зависимости результирующего при-

знака $y$, в роли которого выступает рыночная стоимость (или иной показатель, например, размер арендной ставки), от значений влияющих признаков $x_1, x_2, \ldots, x_k$. При этом, если для большинства объектов движимого имущества можно найти данные о сделках с полными аналогами или отличающимися по какой-либо одной основной характеристике, то на рынке недвижимости практически невозможно подобрать аналоги, совпадающие с объектом оценки по всем существенным характеристикам. Это неизбежно требует использования методов, учитывающих вариации физических и экономических характеристик, местоположения, функционального назначения объектов недвижимости. В настоящее время наиболее часто применяется метод экспертных корректировок, базирующийся в основном на профессиональном опыте и интуиции эксперта-оценщика и, как следствие, имеющий весьма субъективный характер. Ведущими специалистами в области оценочной деятельности [1], [2] не раз отмечалась необходимость снижения субъективности и повышения достоверности результатов практических оценок, чему может способствовать применение в оценочной области математически обоснованных методов, в частности, методов многомерного регрессионного анализа. Исключение составляют случаи, когда объект оценки имеет существенную особенность по какому-то признаку, а по другим для него имеются сопоставимые объекты. В этом случае можно ввести экспертную корректировку $y$, учитывающую эту особенность, а для остальных признаков применить регрессию.

Задачи индивидуальной оценки имеют ряд особенностей, требующих дополнительного рассмотрения. Рынок недвижимости является замкнутым в рамках того или иного территориального образования [3] и, как следствие, в фиксированный промежуток времени на нем имеется информация о весьма ограниченном количестве сделок с близкими аналогами оцениваемого объекта, в особенности для коммерческой и специализированной недвижимости. Поэтому на практике в большинстве случаев стандартные требования к объему $n$ рыночных данных (превышение в 6–7 раз количества влияющих факторов [4], превышение в 5–6 раз [5], превышение как минимум в 4 раза [6]) оказываются невыполнимыми. Данные требования ориентированы на классическую постановку задач статистического моделирования, характерную для массовой оценки, когда главной целью исследования является выявление отдельного влияния каждого из факторов на исследуемую величину (результирующий признак). Применительно к задачам индивидуальной оценки объектов недвижимости такой подход можно считать избыточным. Действительно, основной целью индивидуальной оценки является количественное определение суммарного результирующего влияния основных ценообразующих факторов на значение стоимости (арендной ставки) объекта недвижимости.



Кроме того, при индивидуальной оценке выборка рыночных данных оказывается в определенной степени контролируемой оценщиком, который следит за тем, чтобы в нее попали наиболее близкие к объекту по значениям основных ценообразующих факторов аналоги. Последнее обстоятельство, в частности, позволяет понизить размерность регрессионной модели и увеличить число степеней свободы при фиксированном размере выборки, исключив из модели те факторы, значения которых не меняются или вариации которых несущественны с точки зрения влияния на стоимость.

При отборе аналогов, как правило, фиксируются значения тех признаков, которые могут рассматриваться как классифицирующие для объектов недвижимости. Это, прежде всего, функциональное назначение, часто дополнительно фиксируется тип строения (здания, помещения) и особое местоположение объекта. Количество факторов, значения которых могут быть зафиксированы, зависит от степени активности и открытости рассматриваемого сегмента рынка.

В [7] показано, что при достаточной однородности исходной выборки рыночных данных и хорошей спецификации регрессионной модели можно ограничиться меньшим числом сопоставимых объектов. В эконометрических приложениях регрессионная модель считается вполне адекватной, если значение коэффициента детерминации $R2$ не меньше 0,7 [2], [7] и значение $F$-статистики превышает критический уровень. $F$-статистика является функцией $R2$, поэтому для базового уровня 0,7 можно рассчитать необходимое число степеней свободы и, как следствие, объем выборки, при котором $F$-критерий будет удовлетворителен. При уровне значимости 0,05 значение $F$-статистики превысит критическое для выборок объема $n = 2(k + 2)$, что для 4–7 влияющих факторов составит от 12 до 18 объектов. Если же получаемое значение $R2$ выше, то минимально достаточный для решения задачи индивидуальной оценки объем рыночных данных будет еще меньше.

Другой важной особенностью является необходимость учета в регрессионной модели факторов разной, в том числе и неколичественной, природы. Значения числовых характеристик могут быть как непрерывными, так и дискретными. Неколичественные признаки также могут быть различны: порядковые (качественные) – выраженные в баллах, рангах и характеризующие степень проявления того или иного качества, и номинальные, значения которых не связаны никаким естественным упорядочением, например, описывающие различные классы объектов.

В задачах индивидуальной оценки чаще приходится сталкиваться с порядковыми признаками, поскольку:

– при формировании исходной выборки рыночных данных стараются отобрать сопоставимые объекты недвижимости, принадлежащие, как правило, одному классу;

– эксперт обычно в состоянии высказать экономическую гипотезу о характере влияния значений признака на оцениваемую величину, хотя и не может дать четкого количественного выражения этого влияния.

Из номинальных чаще всего встречаются бинарные признаки, описывающие наличие (отсутствие) какого-либо качества (наличие отдельного входа, парковки и т. п.).

Теория линейных регрессионных моделей с ненулевым свободным членом не накладывает ограничений на характер значений числовых признаков (непрерывные, дискретные). Кроме того, значения (градации признака) инвариантны относительно линейных преобразований, т. е. безразлично, какова точка отсчета и масштаб (цена деления) шкалы [8]. Поэтому неколичественные признаки могут быть учтены в регрессионной модели после присвоения их значениям некоторых числовых меток (оцифровки). Оцифрованные признаки описываются обычно с помощью дискретных шкал с некоторым фиксированным количеством градаций.

Бинарные признаки, т. е. имеющие всего две градации, могут быть оцифрованы произвольным образом, однако из соображений наглядности чаще всего их градациям присваивают значения 0 и 1.

Если признак имеет более двух градаций, то существенным оказывается соотношение расстояний между соседними метками. Так, две линейные регрессионные модели, в одной из которых оцифровка признака «состояние объекта» со значениями «удовлетворительное», «хорошее», «отличное» принята как 1, 2, 3 (соотношение между градациями (3 – 2):(2 – 1), т. е. 1:1), а в другой – 0, 1, 2 (соотношение то же) дадут эквивалентный результат. Однако он не совпадет с результатом модели с оцифровкой этого признака 1, 2, 4 (соотношение (4 – 2):(2 – 1), т. е. 2:1).



Отметим, что еще до этапа оцифровки эксперт-оценщик сталкивается с проблемой выбора градаций неколичественного признака (как номинального, так и порядкового). Выбор должен осуществляться с учетом следующих положений:

– выбору градаций должна предшествовать экономическая гипотеза о характере влияния признака на оцениваемую величину;

– выбор градаций (разбиение на классы) должен производиться на основе существенных различий, оказывающих заметное влияние на значение результирующей величины;

– выбор и упорядочение (для качественных признаков) градаций должны производиться исходя из предполагаемого влияния признака, а не по степени проявления физического свойства объекта.

Например, если при оценке квартир рассматриваются помещения, расположенные на разных этажах, то неправильным было бы в качестве градаций признака «этаж» вводить физический номер этажа: 1, 2, 3, 4, …, поскольку из оценочной практики известно, что различия в расположении на средних этажах не оказывают существенного влияния на значения стоимости квартир. В то же время существенным недостатком квартиры, снижающим ее цену, является расположение на первом и, в меньшей степени, на последнем этаже. Исходя из этого номинальной переменной «этаж» можно сопоставить градации «первый этаж», «средние этажи», «последний этаж». Эти градации можно упорядочить в соответствии с предполагаемым увеличением цены квартир: «первый этаж», «последний этаж», «средние этажи», а признак «этаж» рассматривать далее как качественную переменную.

Существует несколько стандартных процедур оцифровки признаков неколичественной природы.

1. Сведение к совокупности бинарных (булевых) переменных [2], [4], [9], которые в эконометрической литературе чаще называются фиктивными, или искусственными, для оцифровки. Этот метод достаточно универсален, поскольку подходит для оцифровки как номинальных, так и качественных признаков. Кроме того, он объекти-

вен с точностью до количества градаций, поскольку значение градации определяется вкладом фиктивной переменной, т. е. самой регрессионной моделью. Для оцифровки признака с $m$ градациями требуется введение $m - 1$ фиктивной переменной. Если $m$ велико, то переход к фиктивным переменным существенно снижает количество степеней свободы регрессионной модели, что неприемлемо в условиях малой выборки, характерных для задач индивидуальной оценки.Также при небольшом количестве градаций значения фиктивных переменных часто оказываются сильно сопряженными, что может существенно ухудшить качество модели. Поэтому для рассматриваемого класса задач этот подход редко применим на практике.

2. Построение регрессионной модели с фиктивными переменными, а затем выбор в качестве числового значения градации модельной оценки вклада (коэффициента регрессионного уравнения) соответствующей фиктивной переменной [6]. Для этого подхода справедливы аналогичные соображения.

3. Использование равномерного кодирования для качественных признаков, когда расстояние между числовыми метками соседних градаций одинаково, например, «удовлетворительное», «хорошее», «отличное» – 1, 2, 3. Такая кодировка весьма груба и может не отражать реальную степень отличия градаций фактора. Несколько сгладить недостатки, присущие равномерному кодированию, позволяет использование порядковой шкалы качественных оценок [2]. При этом, однако, задание «неравномерности» числовых меток полностью возлагается на эксперта, т. е. весьма субъективно, а в ряде случаев еще и затруднительно.

4. Альтернативой субъективному экспертному подходу является использование оптимизационных процедур [9]–[12] при оцифровке признаков, основанных на максимизации линейной зависимости между влияющей ($x_j$) и зависимой ($y$) переменными. В частности, могут быть использованы следующие критерии, являющиеся взаимосвязанными:

– максимизация коэффициента сопряженности между $x_j$ и $y$;
– минимизация остаточной разности квадратов;
– максимизация коэффициента детерминации $R2$.

Подход на основе оптимизационных процедур также объективен с точностью до количества градаций.



Рассмотренные критерии сами по себе не накладывают никаких ограничений на порядок следования градаций признака, поэтому после оцифровки он может измениться. Для номинальных признаков и в случае, если порядковая переменная отражает лишь степень проявления некоторого качества объекта недвижимости безотносительно к его влиянию на зависимый признак, изменение порядка следования градаций не критично. Однако, если первоначальные метки градациям были назначены экспертом-оценщиком исходя из экономической гипотезы влияния на результирующий признак, изменение их следования может свидетельствовать о неправильном выборе градаций признака или спецификации регрессионной модели.

В [10] для оцифровки признаков предложено использовать оптимизационные процедуры **Поиск решения** MS Excel. Вместе с тем для линейной регрессионной модели известен прозрачный метод оптимизации, не требующий сложных вычислений. Он заключается в том, что каждой градации $x_j^q$ признака $x_j$ ставится в соответствие среднее арифметическое значений $y_i$ зависимого признака по всем объектам, которые имеют то же значение градации $x_{ij} = x_j^q$. Пусть в исходной выборке данных, состоящей из $n$ объектов, набралось $n_q$ объектов, у которых значение рассматриваемого фактора совпало с градацией $x_j^q$. Тогда этой градации можно присвоить числовую метку $\tilde{x}_j^q$,

$$\tilde{x}_j^q = \frac{1}{n_q} \sum_{x_{ij}=x_j^q} y_i . \qquad (1)$$

Такая перекодировка хорошо интерпретируема и максимизирует корреляцию $y$ и $x_j$. Вместе с тем она применима лишь для факторов, оказывающих наиболее значимое влияние на $y$. Для второстепенных признаков, влияние которых на $y$ прослеживается не столь явно, полученные по формуле (1) числовые метки могут противоречить экономическому смыслу. В этом случае рекомендуется использовать метод последовательного числового перекодирования [9], [11]. Пусть построена регрессионная модель, в которую включены все необходимые количественные, бинарные и наиболее влияющие неколичественные признаки, оцифрованные по формуле (1). Тогда в качестве числовых меток для градаций второстепенного влияющего фактора можно рассмотреть средние арифметические остатков $\varepsilon_i$ (2).

Таким образом, рассматривается влияние этого признака на еще не объясненную моделью часть наблюдаемых ценовых значений. Такая перекодировка минимизирует остаточную разность квадратов.

$$\tilde{x}_j^q = \frac{1}{n_q} \sum_{x_{ij}=x_j^q} \varepsilon_i, \qquad (2)$$

где $\varepsilon_i = y_i - \hat{y}_i$ – разности между наблюдаемыми и модельными значениями результирующего признака.

В случае значительного (в несколько порядков) различия в масштабах шкал для разных признаков может оказаться существенной инструментальная ошибка (погрешность вычислений), вызванная плохой обусловленностью регрессионной матрицы. Поэтому завершающим этапом оцифровки признаков является масштабирование их количественных значений.

Следует помнить, что решаемая задача носит прикладной характер, поэтому применение процедур оцифровки не должно нарушать экономического смысла.

### Литература


1. *Грибовский С. В., Сивец С. А., Левыкина И. А.* Новые возможности сравнительного подхода при решении старых проблем // Вопросы оценки. 2002. № 4. С. 22–29;
2. *Сивец С. А., Левыкина И. А.* Эконометрическое моделирование в оценке недвижимости. Запорожье: Полиграф, 2003.
3. *Грибовский С. В.* Оценка доходной недвижимости. СПб.: Питер, 2001.
4. Эконометрика: Учебник / Под ред. И. И. Елисеевой. М.: Финансы и статистика, 2001.
5. Теория статистики / Под ред. проф. Р. А. Шмойловой. М.: Финансы и статистика, 1998.
6. Отчет «Разработка методики определения уровня арендной платы за нежилые помещения в Санкт-Петербурге». СПб.: Администрация Санкт-Петербурга, КУГИ, ГУИОН, 1997.
7. *Анисимова И. Н., Баринов Н. П., Грибовский С. В.* О требованиях к количеству сопоставимых объектов при оценке недвижимости сравнительным подходом // Вопросы оценки. 2003. № 1.
8. *Магнус Я. Р., Катышев П. К., Пересецкий А. А.* Эконометрика. Начальный курс: Учеб. 5-е изд., испр. М.: Дело, 2001.
9. *Котюков В. И.* Многофакторные кусочно-линейные модели. М.: Финансы и статистика, 1984.





10. *Андреев Д. М.* Оптимизационная модель назначения балльных оценок значениям ценообразующих факторов // Вопросы оценки. 2002. № 3.
11. *Котюков В. И.* Некоторые нестандартные статистические модели прогнозирования в эконометрии. Новосибирск: НИЖТ, 1977.
12. *Енюков И. С.* Методы оцифровки неколичественных признаков // Алгоритмическое и программное обеспечение прикладного статистического анализа. М.: Наука, 1980.


УДК 378.001.658.011.56

**© А. М. Грушко**

Санкт-Петербургский государственный инженерно-экономический университет

## ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРИ ОПРЕДЕЛЕНИИ ВЛИЯНИЯ ИЗМЕНЕНИЯ ТАРИФОВ НА ЭЛЕКТРИЧЕСКУЮ И ТЕПЛОВУЮ ЭНЕРГИЮ НА ЭКОНОМИКУ

Главные экономические, организационные и правовые основы государственного регулирования тарифов на электрическую и тепловую энергию (ЭиТЭ) в Российской Федерации определены Федеральным законом РФ «О государственном регулировании тарифов на электрическую и тепловую энергию в Российской Федерации». Изменение тарифов может происходить не чаще одного раза в год, и максимальная величина изменения также ограничена. Способность оценить последствия изменения тарифов, которые могут произойти в результате осуществления деятельности государства по их регулированию, становится важной задачей в условиях нестабильной экономической обстановки.

Чтобы решить такую задачу, необходимо иметь достоверную, полную и надежную информацию о реакции экономики на ценовое влияние меняющихся энерготарифов. Если сведения о характере изменений в тарифах являются публичным достоянием, то проследить результаты воздействия на экономику гораздо сложнее. Следует учитывать ряд обстоятельств:

– информационную асимметричность при изменении тарифов;
– фактическое упреждающее ценообразование в бизнесе;
– вероятное искажение будущих изменений.

Потребители на рассматриваемом товарном рынке обладают существенными различиями в поведении в силу своих институцио-

нальных особенностей. Поэтому изучать влияние изменяющихся цен на их реакцию следует, предварительно определив типы потребителей и их отличия в характере реагирования. По принципам реагирования на изменяющиеся тарифы на ЭиТЭ можно выделить отдельные группы:

– предприятия промышленности, транспорта, сельского хозяйства;

– население.

Хотя для промышленных предприятий, транспорта и АПК устанавливаются различные тарифы, в экономике страны они участвуют в производстве валового национального продукта и включены в систему межотраслевого взаимодействия. Оказывается, что без учета межотраслевого взаимодействия оценить влияние тарифов на ЭиТЭ можно только в теоретическом случае существования отрасли промышленности, не использующей в своем технологическом цикле продукцию других отраслей, или в случае жесткого фиксирования цен на продукцию.

Идеология межотраслевого взаимодействия находит отражение в системе таблиц «Затраты–Выпуск», содержащих подробные характеристики производства и использования товаров и услуг, а также доходов, формирующихся в процессе производства. Систематически выпускаемые Госкомстатом России сборники показателей системы национальных счетов совершенствуются. Однако для решения практических задач информацию, извлеченную из официального источника, гарантирующего ее надежность, необходимо подвергать обработке. На основе предложенной методики были произведены расчеты с использованием пакета программного обеспечения Microsoft Office, в частности математического инструментария MS Excel.

*Методический подход к оценке влияния изменения тарифов на ЭиТЭ на цены конечной продукции.* Экономические взаимосвязи в сфере производства товаров и услуг отражаются в системе национального счетоводства (СНС) на основе идеологии межотраслевых балансов (МОБ). Схема МОБ состоит из трех основных частей, называемых квадрантами, отличными по экономическому содержанию (рисунок).

I квадрант характеризует производственные взаимосвязи типа «продукт–отрасль». Отрасль представляет собой совокупность предприятий и организаций, принадлежащих соответствующей отрасли



действующего в настоящее время ОКОНХ. Под продуктом понимается совокупность однородных товаров и услуг данного вида, произведенных в различных отраслях экономики. Каждый элемент I квадранта ($a_{ij}$), отражает затраты $i$-го вида товара (услуги) на производство продукции $j$-й отрасли.

| | |
|---|---|
| Промежуточное потребление (I квадрант) $\mathbf{A} = \| a_{ij} \|$ | Конечное использование (II квадрант) $\mathbf{Y} = \| y_{im} \|$ |
| Добавленная стоимость (III квадрант) $\mathbf{C} = \| c_{ik} \|$ | |

Схема межотраслевого баланса

II квадрант показывает конечное использование выделенных групп товаров и услуг по категориям (расходам на конечное потребление, валовое накопление и экспорт). Каждый элемент II квадранта ($y_{im}$) обозначает, сколько товара $i$-й отрасли идет на потребление $m$-й категорией.

III квадрант характеризует состав валовой добавленной стоимости (оплату труда, валовую прибыль, валовый смешанный доход, другие налоги на производство, другие субсидии на производство) по отраслям экономики. Каждый элемент III квадранта ($c_{kj}$), показывает $k$-й источник формирования добавленной стоимости $j$-й отрасли.

Если рассматривать I квадрант МОБ по вертикали, то в каждом столбце показывается стоимостная структура выпуска отдельных отраслей. В продолжение вертикали располагается III квадрант, где видна добавленная стоимость по каждой отрасли. Таким образом, структура цены продукта $j$-й отрасли формируется как сумма всех затрат на производство и добавленной стоимости.

$$\sum_i a_{ij} + c_j = 1, \ \forall j. \qquad (1)$$

Выражение (1) означает, что производство $j$-й отрасли представлено затратами на все виды необходимых материалов, $a_{ij}$, произведенных всеми другими отраслями, и добавленной стоимостью $c_j$.

Матрица полных затрат отражает, сколько надо затратить продукции $i$-й отрасли, необходимой не только для производства $j$-й от-

расли, но и для собственного потребления $i$-й отраслью. Таким образом, полные затраты будут всегда больше затрат прямых.

$$\mathbf{B} = (\mathbf{E} - \mathbf{A})^{-1}, \qquad (2)$$

где **E** – единичная матрица, число строк и столбцов которой равно числу отраслей и соответствующих им товаров и услуг.

Когда из МОБ вытекает представление о технологических связях между отраслями, цены в нем должны быть фиксированными, чтобы выступать лишь в роли измерителя объема продукта.

Стандартное соотношение баланса цен будет иметь следующий вид:

$$\mathbf{p} = \mathbf{wC}(\mathbf{E} - \mathbf{A})^{-1} = \mathbf{wCB}, \qquad (3)$$

где **w** – вектор цен факторов добавленной стоимости.

Если все продукты и факторы представлять в стоимостной форме, то цены товаров будут равны единице. Также будут равны единице и цены факторов. Тогда по сравнению с исходным балансом можно будет судить о любых изменениях. Изменения цен факторов или их использования в отраслях приведут к нарушению равенства (1), поэтому можно будет обнаружить не абсолютные, а относительные изменения.

Для определения влияния изменения энергетического тарифа на цены конечных продуктов по отраслям промышленности добавим специальную дополнительную строку в III квадрант матрицы **C**, в которой теперь будет 2 строки. Сами цены на продукцию отраслей будут выражены отраслевыми индексами цен (по отношению к базовым уровням).

Поскольку изменение цен происходит на продукцию лишь одной отрасли, энергетической, во вновь введенной строке «изменение цен» для всех отраслей значения коэффициентов будут нулевыми, и только в первой позиции, соответствующей отрасли, производящей ЭиТЭ, появится $\delta$. Тогда можно выделить следующие свойства решения:

а) все индексы цен – линейные двучлены относительно $\delta$;

б) свободные члены равны 1 (когда цена на электроэнергию не меняется, $\delta = 0$, все цены остаются такими, какими были в исходном балансе, $p_j = 1$);

в) строка коэффициентов при $\delta$ – строка матрицы полных затрат, соответствующая затратам электроэнергии в отраслях.



Остается только определить изменение цен, которое для продукта $j$-й отрасли можно представить как

$$p_j = 1 + b_j\delta, \qquad (4)$$

где $p_j$ – индекс цен на продукцию $j$-й отрасли,

$b_j$ – коэффициент полных затрат $j$-й отрасли,

$\delta$ – относительное изменение энергетического тарифа.

Изменение цены продукта будет определяться коэффициентом при $\delta$. Если ввести обозначение $\delta_j$ для относительного прироста этой цены,

$$p_j = 1 + \tau_j, \qquad (5)$$

то в нашем примере

$$\tau_j = \frac{\tau_э b_j}{b_э}, \qquad (6)$$

т. е. относительный прирост цены продукта $j$-й отрасли будет получаться произведением относительного прироста энергетического тарифа на отношение коэффициента полных затрат отрасли к коэффициенту полных затрат электроэнергетики.

*Оценка влияния изменения тарифов на ЭиТЭ в будущем периоде.* Изменение цен на продукцию отраслей промышленности происходит по-разному и находит отражение в индексах цен на соответствующую продукцию, публикуемых Госкомстатом РФ в ежегодных сборниках. Предложенная методика оценки влияния изменения тарифов на электрическую и тепловую энергию на цены конечной продукции основана на системе межотраслевого взаимодействия, не подверженной воздействию изменения цен в краткосрочном периоде. Экономическая система в целом может характеризоваться темпами инфляции, официально публикуемыми как индекс-дефлятор.

Как и для населения, в отношении промышленных предприятий может быть применен подход, учитывающий инфляционные процессы. Необходимо сравнить планируемый рост тарифов с последними сведениями об инфляции. Если рост тарифов будет отставать от темпов инфляции, то влияние на цены будет ослабевать, при совпадении роста тарифов с темпами инфляции – сохранится равновесие. Только превышение темпов тарифного роста над уровнем инфляции может привести к росту цен конечной продукции.

Приняв допущение о сохранении инфляционной тенденции в будущем периоде, можно оценить влияние тарифного роста на цены

конечной продукции. Произведение разницы темпов роста тарифов и инфляции на коэффициенты относительного роста цен на продукцию по отраслям промышленности отразит величину влияния изменения тарифов на ЭиТЭ на цены конечной продукции.

Объединив подходы для оценки тарифного воздействия на население и предприятия, получим комплексную методику, благодаря которой становится возможным решение проблемы в масштабах всей экономики. Одним из наиболее значимых факторов этого является качественное информационное обеспечение. Практическая ценность работы состоит в определении источников и способов получения достоверной, полной и надежной информации.

УДК 378.001.658.011.56

© О. Б. Кузнецова

Санкт-Петербургский государственный
инженерно-экономический университет

## ОРГАНИЗАЦИОННОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ЦЕНТРОВ ДОВУЗОВСКОГО ОБРАЗОВАНИЯ

Система довузовского образования играет важную роль во всей системе образования Российской Федерации. Особенно четко это проявляется в новых экономических условиях в связи с ярко выраженным дисбалансом рынка образовательных услуг и рынка труда.

Традиционно термин «довузовское образование» используют применительно к образовательным услугам, получаемым учащимися старших классов образовательных учреждений разного типа сверх базисного учебного плана, как правило, при прямом или косвенном участии в образовательном процессе высших учебных заведений, а также на подготовительных курсах, факультетах довузовской подготовки в вузах.

Система довузовского образования, с одной стороны, является промежуточным звеном между системами среднего полного и высшего профессионального образования, а с другой стороны, является встроенной в систему высшего профессионального образования. Причем довузовское образование рассматривается как начальный этап подготовки специалистов с высшим профессиональным образованием.



Одна из наиболее важных на сегодняшний день задач, которые ставит перед собой система довузовского образования, – научить школьников думать самостоятельно. Это означает не только запоминать правила и формулировки, но и уметь рассуждать и анализировать, т. е. обладать тем уровнем знаний, умений и навыков, которые обеспечивают возможность получения высшего профессионального образования (в том числе и в ускоренные сроки).

Таким образом, традиционная образовательная функция довузовского образования заключается в приведении образовательного уровня абитуриента в соответствие с требованиями вступительных испытаний в вуз.

В настоящее время можно выделить обобщенную схему взаимодействия общего, среднего профессионального и высшего образования (рис. 1).

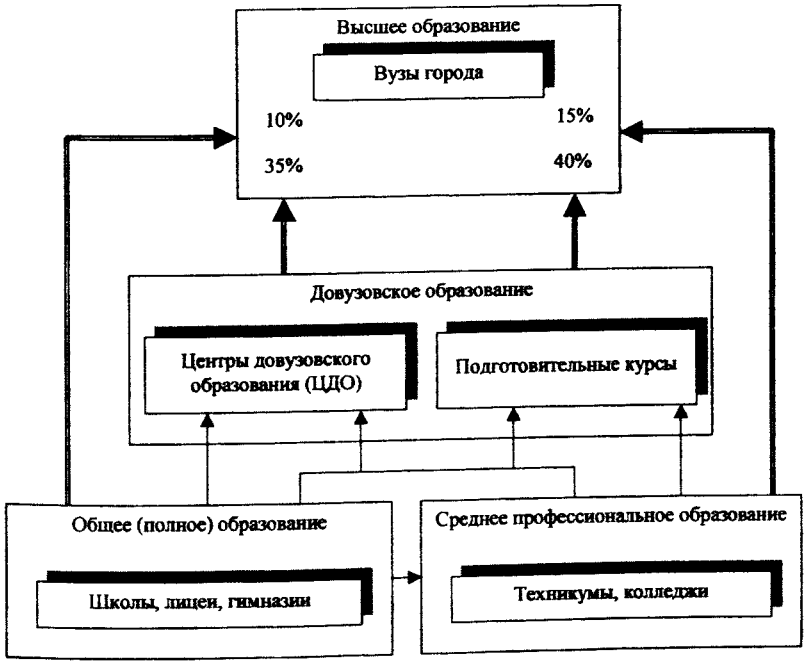



**Рис. 1. Обобщенная схема взаимодействия общего, среднего профессионального и высшего образования**

Как видно из рис. 1, число поступивших напрямую из школ составит около 10% от общего числа поступивших в вуз, техникумов – 15%, остальная же часть принадлежит системе довузовской подготовки для поступления в конкретный вуз. При этом величина поступивших с подготовительных курсов составит в среднем 40%, а с центров довузовского образования (ЦДО) – 35%.

Система довузовского образования представляет собой сложную территориально-распределенную систему, основным элементом которой являются структуры, реализующие программы довузовского образования ЦДО.

Деятельность ЦДО осуществляется при наличии лицензии на ведение образовательной деятельности, непосредственно у центра или у предприятия, учреждения, организации, в рамках которой он функционирует.

ЦДО могут являться:

– самостоятельными юридическими лицами любой организационно-правовой формы, предусмотренной законодательством;

– подразделениями предприятий, учреждений, организаций любой организационно-правовой формы, предусмотренной законодательством, для которых образовательная деятельность – не основной вид деятельности;

– подразделениями образовательных учреждений любой организационно-правовой формы, предусмотренной законодательством, реализующими программы дополнительного образования;

– подразделениями образовательных учреждений любой организационно-правовой формы, предусмотренной законодательством, реализующими образовательные программы начального и среднего профессионального образования.

Это приводит к реализации в рамках довузовского образования обучения по вузовским программам профилирующих дисциплин, адаптированных к требованиям образовательных программ среднего образования в качестве базового уровня и учитывающим возрастные особенности учащихся.

Такой подход позволяет решить проблему ускоренного высшего профессионального образования за счет более раннего изучения ряда профилирующих дисциплин (с их последующим перезачетом после необходимой проверки знаний в вузе), а также за счет реализации более интенсивного графика учебного процесса в вузе.



Ассоциация «Экономика – АЛЬМА» осуществляет формирование системы довузовского экономического образования с 1991 г. Она осуществляет интеграцию деятельности Санкт-Петербургского государственного инженерно-экономического университета и ЦДО, организацию и управление системой довузовского образования, а также ее расширение и развитие. Ассоциация выполняет роль своего рода координационного центра, и ей университетом делегированы полномочия в области формирования контингента абитуриентов по сокращенным срокам обучения по специальностям «Коммерция» и «Прикладная информатика в экономике». На рис. 2 представлена схема работы НОУ Школы бизнеса «Экономика – АЛЬМА» (НОУ ШБ).

ЦДО как в регионах, так и в Санкт-Петербурге организуют двухлетнее обучение школьников (10–11 классы) по специальным рабочим программам (углубленная школьная и частичная программа вуза) по согласованному рабочему плану – экономика, информатика, высшая математика.

Обучение для школьников платное, оплата покрывает расходы ЦДО. От довузовской части Школа бизнеса «Экономика – АЛЬМА» получает доход только в виде оплаты за учебные пособия, задачники, а также оплачиваются выезды представителей ШБ для проведения тестирования (для иногородних центров прибыль, если она есть, остается в этих центрах, в Санкт-Петербурге довузовское образование организуется на уровне «самоокупаемости»).

«Экономика – АЛЬМА» организует методическое руководство и помощь в работе ЦДО:

– разработку учебных планов, рабочих программ дисциплин;

– разработку методических указаний для преподавателей, учебных пособий, задачников;

– проведение ежегодных конференций в Санкт-Петербурге для руководителей и преподавателей ЦДО;

– консультации для преподавателей ЦДО;

– проведение ежегодных контрольных работ и тестирования учеников (10–11 классы) с выездом представителей НОУ ШБ «Экономика – АЛЬМА» в ЦДО;

– проведение деловых игр в крупных ЦДО (с элементами профориентации и агитации).

Приемная комиссия университета организовывает выездные комиссии для проведения приемных испытаний в иногородних ЦДО

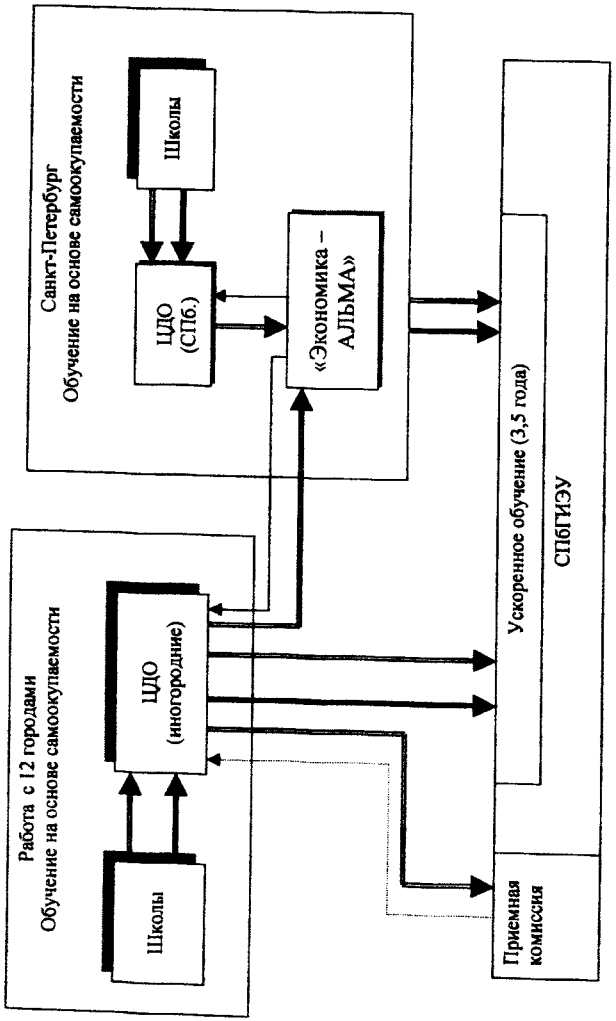



Рис. 2. Схема работы НОУ ШБ «Экономика – АЛЬМА»:
– направление учащихся на обучение;
– оплата деятельности;
– выездные приемные комиссии;
– методическое руководство



(на ускоренное обучение 3,5 и 5 лет) и др. Иногородние ЦДО оплачивают выезд представителей приемной комиссии.

Поступающие в СПбГИЭУ на ускоренное (3,5 года) обучение выпускники ЦДО заключают договор с университетом на обычной для коммерческой формы обучения основе.

За 11 лет совместной работы налажены личные контакты с руководителями ЦДО, отработана технология работы, накоплен опыт и методические наработки по всем направлениям работы.

Учитывая вышеизложенное, представляется целесообразным проанализировать подобный опыт взаимодействия систем среднего и высшего образований через систему довузовского образования. Необходимо выявить проблемы, возникающие в деятельности ЦДО и предложить эффективные методы их решения.

Радикальные изменения в среде бизнеса требуют новых взглядов на организацию деятельности центров довузовского образования (ЦДО), новых принципов ее построения и новых подходов к управлению.

Поэтому многие российские ЦДО сталкиваются с серьезными проблемами:

– мониторинг коммерческой деятельности учреждения довузовского образования (как коммерческой деятельности в целом, так и ее отдельных направлений);

– формирование портфеля заказов на образовательные услуги (возникла полная нестыковка предложений со стороны вузов и потребностей на рынке труда);

– прогнозирование жизненного цикла предоставляемых образовательных услуг;

– учет способностей учащихся и содержания изучаемых ими дисциплин;

– вопросы стратегического и оперативного управления.

Немаловажным становится вопрос подбора кадров для преподавания в ЦДО – будут это преподаватели вузов (прекрасно владеющие программой того или иного вуза) или же учителя школ (знакомые с психологией учеников).

Безусловно, актуален вопрос оплаты труда преподавателей подобных учреждений довузовского образования.

Остро стоит вопрос о разработке системы, позволяющей давать сравнительную оценку деятельности образовательных учреждений системы довузовского образования отдельного региона и страны в целом, обеспечить информационную поддержку тех или иных ЦДО на рынке образовательных услуг.

Таким образом, необходимо оптимальное решение указанных задач, возникающих в деятельности учреждения довузовского образования на основе математических и инструментальных методов.

УДК 378.001.658.011.56

© А. А. Лепихин

Санкт-Петербургский
государственный университет

## КОНВЕРТИРОВАНИЕ СТАНДАРТНЫХ КАДРОВ В ОТЕЧЕСТВЕННЫХ СЕТЕВЫХ КОНЦЕНТРАТОРАХ

В начале 2003 г. в нашей стране была закончена разработка нового сетевого концентратора. Представленная модель содержала 28 портов Ethernet и два порта FDDI. Данный концентратор является самым мощным из отечественных сетевых устройств.

Одна из проблем при разработке сетевого концентратора – проблема преобразования протоколов канального уровня по классификации модели OSI (Open System Interconnection). Рассмотрим, как была решена возникшая проблема.

Каждый кадр имеет заголовок, блок данных и «хвост». Чтобы правильно конвертировать кадры, необходимо знать формат заполнения всех полей заголовка кадров и способы их вычисления. Как правило, заголовок кадра содержит адреса, представленные в определенном формате, поля «Тип кадра», «Длина кадра» и контрольные поля.

Согласно международным стандартам по сетевым технологиям кадры типа FDDI_SNAP и Ethernet_II используются для передачи пользовательских данных, для служебных данных используются другие типы кадров. Кроме того, эти кадры являются взаимно конвертируемыми. Поэтому они и были выбраны объектом внимания разработчиков концентратора.



Ниже приведены их форматы (рис. 1).

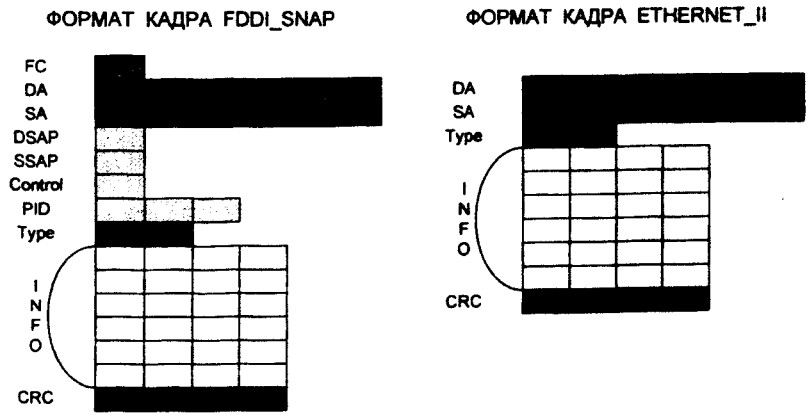



Рис. 1. Форматы кадров

Разберем поля кадров:

– FC (Контроль кадра), 1 байт, для кадра с данными имеет значение 57h,

– DA (Адрес назначения), 6 байт,

– SA (Адрес отправителя), 6 байт,

– DSAP, SSAP, Control, PID (Поля вышестоящего протокола), 6 байт,

– Type (Тип), 2 байта,

– INFO (Данные), от 46 до 1 500 байт,

– CRC (Контрольная сумма), 4 байта, вычисляется по специальному алгоритму.

Непосредственно конвертирование кадра FDDI_SNAP в кадр Ethernet_II происходит следующим образом: сначала из FDDI_SNAP вырезаются поля FC, DSAP, SSAP, Control и PID, причем присутствие поля в обоих типах кадров отнюдь не означает, что при конвертировании значение поля будет просто перенесено. Поле может быть вычислено как исходя из значения аналогичного поля в другом кадре, так и исходя из значений всех полей кадра. Затем конвертируются адресные поля, для этого в каждом байте адреса меня-

ется порядок следования битов, т. е. байт переворачивается. Поля Type (Тип) и INFO (Данные) просто переносятся в тело другого кадра. Поле контрольной суммы (CRC) вообще не подлежит конвертированию. Для его вычисления полученный кадр пропускают через алгоритм 32-битного нахождения контрольной суммы, который называется CRC_32.

Конвертирование кадра Ethernet_II в кадр FDDI_SNAP происходит с точностью до наоборот. Перед началом получаемого кадра ставится поле FC со значением 57h, затем преобразуются адреса путем переворачивания каждого байта; добавляются поля DSAP = AAh, SSAP = AAh, Control = 03h, PID = 00 00 00h, переносятся без изменений Type и INFO и, наконец, вычисляется контрольная сумма.

Данный механизм представляется достаточно простым, так как здесь есть только одно поле, значение которого зависит от всего кадра, – это поле CRC (контрольная сумма). К тому же оно является последним полем, что позволяет конвертировать кадры в режиме непрерывного потока, т. е. слово за словом, байт за байтом. Однако необходимо понимать следующее: кадр проходит не только через систему вырезания/добавления полей, но одновременно и через систему вычисления контрольной суммы. В свою очередь эти две системы контролируются системой-менеджером, которая обеспечивает непрерывность потока и компенсацию задержки вычисления контрольной суммы. Кроме того, все это должно выполняться в реальном времени, а это значит, что при обработке кадра ни при каких условиях *не должны* накапливаться задержки; иначе это приведет к перегрузке системы!

На рис. 2 показан временной отрезок прохождения кадра. Вырезав ненужные поля, получим дырявый кадр, чтобы склеить его в непрерывный поток, необходим сквозной буфер, через который прокачивается весь кадр (рис. 3). Причем по мере вырезания полей точка считывания из буфера будет приближаться к точке записи. Аналогично при добавлении полей используется буфер запаса (рис. 4). Но точка считывания постепенно удаляется от точки записи. Объемы буферов жестко зависят от размеров добавляемых/вырезаемых полей и от задержки вычисления контрольной суммы.



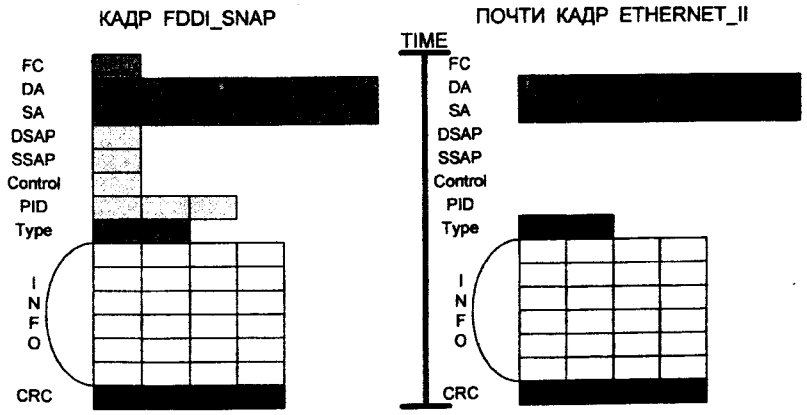



Рис. 2. Конвертирование кадров

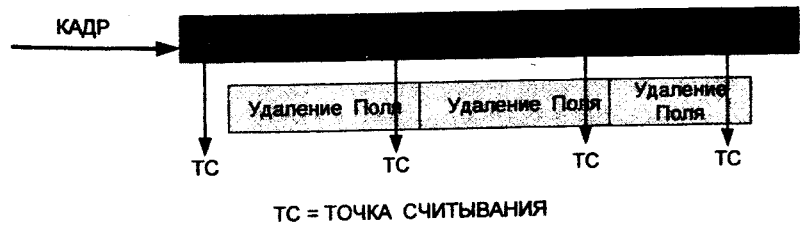



Рис. 3. Сквозной буфер

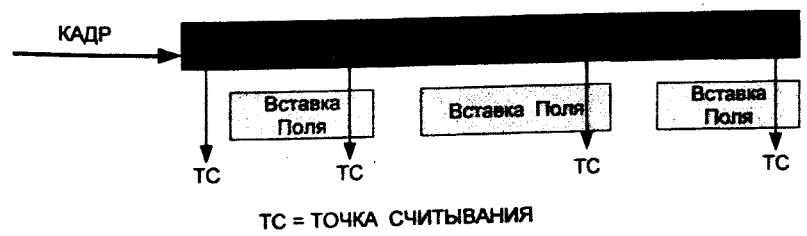



Рис. 4. Буфер запаса

Такая схема создает фиксированное временное смещение обработанного потока кадров и позволяет избежать накопления задержек конвертирования.

УДК 378.001.658.011.56

© А. А. Лепихин

Санкт-Петербургский
государственный университет

# ПРЕОБРАЗОВАНИЕ СЛУЖЕБНЫХ КАДРОВ В ОТЕЧЕСТВЕННЫХ СЕТЕВЫХ КОНЦЕНТРАТОРАХ

Кадры типа FDDI_RAW и Ethernet_RAW используются для передачи служебных данных о состоянии устройств в сети, для пользовательских данных используются другие типы кадров. Чтобы конвертировать эти кадры, необходимо знать не только механизм замены полей, но и некоторые дополнительные особенности. Рассмотрим их форматы (рис. 1).

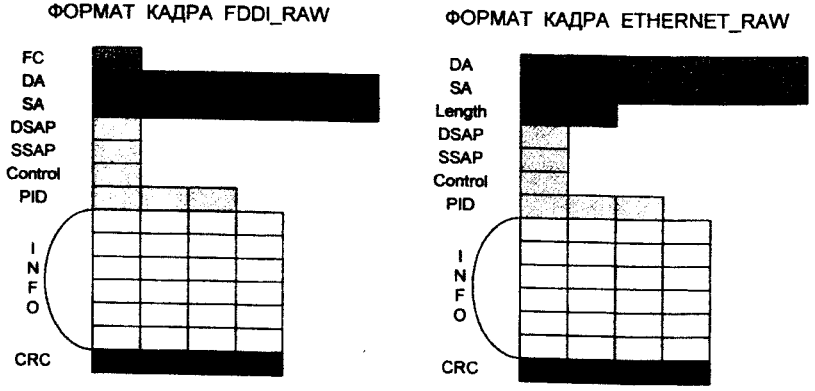



Рис. 1. Форматы кадров

Поля кадров:

– FC (Контроль кадра), 1 байт, для кадра с данными имеет значение 57h;

– DA (Адрес назначения), 6 байт;

– SA (Адрес отправителя), 6 байт;

– DSAP, SSAP, Control, PID (Поля вышестоящего протокола), 6 байт;

– Length (Длина кадра), 2 байта;



– INFO (Данные), от 46 до 1500 байт;

– CRC (Контрольная сумма), 4 байта, вычисляется по специальному алгоритму.

Чтобы правильно провести преобразование кадра Ethernet_Raw в кадр FDDI_RAW, необходимо распознать пришедший кадр. Но начинается преобразование с добавления поля FC, затем путем переворачивания каждого байта конвертируются адреса. Анализ поля Length дает возможность распознать тип кадра. Если значение меньше 1 000h, то это кадр Ethernet_Raw, иначе Ethernet_II. Итак, если пришедший кадр есть Ethernet_Raw, то далее передаются поля DSAP, SSAP, Control, PID и INFO, в противном случае включается алгоритм преобразования кадра Ethernet_II, который здесь не рассматривается. В конце выдается значение контрольной суммы, которое вычисляется по алгоритму CRC_32 исходя из значения каждого слова кадра.

При длине данных Ethernet_Raw кадра менее 48 байт он автоматически дописывается значениями 02h в поле INFO до длины 64 байта, в то время как FDDI_RAW кадр не имеет такого ограничения. Поэтому, обнаружив такой короткий Ethernet кадр и конвертируя его в FDDI, придется отбросить ненужные байты в поле INFO. Число полезных байт в поле данных вычисляется по простой формуле 48–Length.

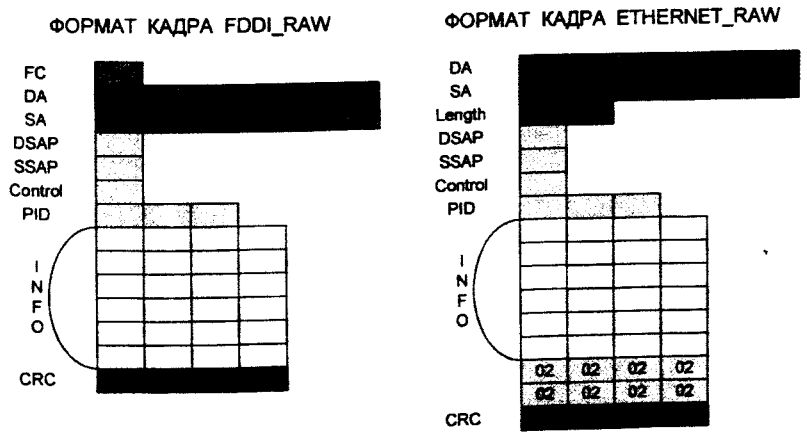



Рис. 2. Конвертирование кадров

Преобразование кадров происходит в режиме непрерывного потока, т. е. слово за словом. Это крайне важно в системах реального времени, поскольку позволяет избежать накопления задержек обработки кадров.

Обратное конвертирование (из FDDI_RAW в Ethernet_Raw) содержит другую немаловажную особенность, связанную с полем длины кадра. Само преобразование происходит аналогично описанному выше (см. рис. 2). Вырезается поле FC, переворачиваются байты адресов и т. д. Узнав значение поля DSAP, можно выбрать алгоритм дальнейшего конвертирования. Если DSAP = AAh, то результатом будет кадр Ethernet_II, иначе Ethernet_Raw. Для получения Ethernet_Raw передаются поля всех данных (DSAP, SSAP, Control, PID и INFO) и считается их общая длина. В случае если длина меньше 48, вслед за данными передается несколько (48–Length) байт со значением 02h.

Таким образом, после первой стадии конвертирования получается кадр Ethernet_Raw, но в поле Length отсутствует значение. При этом сам кадр уже находится в промежуточном блоке памяти, здесь удобно использовать FIFO (рис. 3). Поскольку весь кадр уже прошел первую стадию, нам стала известна его длина, которая немедленно передается в блок второй стадии конвертирования. Второй блок выполняет алгоритм вычисления контрольной суммы и заполняет поле длины. По сути FIFO выполняет роль сквозного буфера для целого кадра. Сквозной буфер необходим для поддержания режима непрерывного потока.

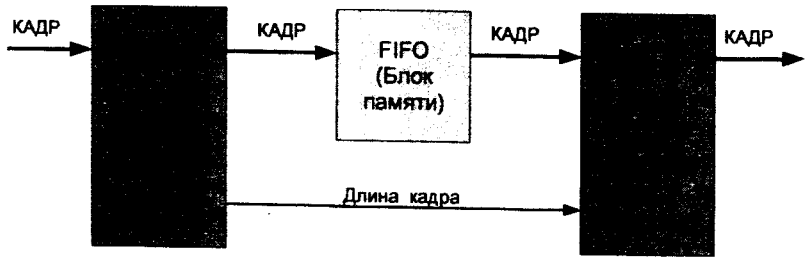



Рис. 3. Стадии конвертирования

Согласно международным стандартам на протокол Ethernet, длина кадра не превышает 1 520 байт. Поэтому размер FIFO жестко



устанавливается на 1,5 килобайта. К сожалению, фиксированной задержки кадров на выходе из конвертора избежать невозможно.

УДК 378.001.658.011.56

© А. М. Петрова, А. В. Сербин
Санкт-Петербургский государственный инженерно-экономический университет

## ЭЛЕКТРОННЫЕ СИСТЕМЫ ПОДДЕРЖКИ ИСПОЛНЕНИЯ

В настоящее время, в век информации, организации сталкиваются с постоянно возрастающей информационной волной. Если организация стремится оставаться конкурентоспособной, она должна осваивать новые пути сбора и хранения информации, а также доступа к ней из внешней и внутренней среды. Также существует необходимость собирать как индивидуальные знания сотрудников организации, так и знания, созданные самой организацией, с целью предоставления этих знаний другим сотрудникам и самой организации для выполнения текущих рабочих задач[1] и приспособления к изменениям окружающей среды. Создавая электронную инфраструктуру, организация может собирать информацию и опыт бывших и настоящих работников. Электронные системы поддержки исполнения (EPSS) – это инструмент для сбора информации, накопления опыта в организации и создания благоприятной среды для обучения. EPSS могут также использоваться как ядро сетевой систематизации знаний сотрудников [2].

### *Определение электронных систем поддержки исполнения*

Существует множество определений ESPP, однако, приведем здесь определение из фундаментального труда Глории Джери (Gloria Gery) «Электронные системы поддержки исполнения», опубликованном в 1991 г. EPSS здесь определяются как «интегрированная электронная среда, легко доступная каждому сотруднику и структурированная для предоставления немедленного индивидуального on-line доступа к полному набору информации, программного обеспечения, руководств, советов и помощи, данных, графических средств, инст-

[1] Понятие «рабочие задачи» включает в себя функции решения проблем, принятие решений, планирование и информационное управление.

рументов, систем оценки и мониторинга, для исполнения его [сотрудника] функций с минимальной поддержкой и вмешательством других сотрудников» [1].

Электронные системы поддержки исполнения могут быть описаны как любое компьютерное программное обеспечение или компонент, который повышает эффективность исполнения работником его функций:

– уменьшая сложность или число действий, требуемых для исполнения задания;

– предоставляя информацию, необходимую работнику для исполнения задания;

– предоставляя систему поддержки принятия решений, которая позволяет работнику определить действие для особой совокупности условий.

Электронные системы поддержки исполнения могут помочь организации уменьшить затраты на обучение персонала, повышая продуктивность и эффективность исполнения. Они могут позволить работнику выполнять задания с минимальным количеством внешнего вмешательства и обучения. Используя такой тип систем, работник, особенно новичок, сможет не только выполнить свою работу быстрее и аккуратнее, но и больше узнать о своей работе и о работе всей организации [4].

### *Проблемы, решаемые с помощью EPSS*

EPSS, дружественные и простые в использовании, – визуальные инструменты, которые делают сложные задания простыми.

Макросы, мастера, шаблоны и другие инструменты электронной поддержки исполнения однозначно дают немедленный и эффективный толчок к исполнению, причем на высоком уровне качества.

Не удивительно, что они также предоставляют решения таких острых организационных проблем, как:

– необходимость в стандартизации;

– высокая текучесть кадров;

– сокращение персонала, обслуживающего информационные системы;

– дорогостоящее и многостороннее технологическое обучение.

В табл. 1 показана эффективность использования EPSS при решении этих и некоторых других проблем [5].



Таблица 1

**Эффективность исследования EPSS**

| Проблема | Польза от EPSS |
|---|---|
| Необходимость стандартизации всей документации | Стандартизация осуществляется за счет использования шаблонов (без использования ручного форматирования) |
| Бумажные документы и формы | Автоматизация документации с использованием шаблонов и мастеров увеличивает исполнение и продуктивность |
| Растущий массив корпоративного опыта и знаний | Знания, нужные для выполнения сложного задания, вложены в инструмент и просто распределяются между работниками |
| Необходимость в увеличении результативности и эффективности исполнения | Завершение задания рационализировано и исключает необходимость изучать полностью работу всего ПО |
| Высокая текучесть кадров | Знания, необходимые для выполнения сложного задания, должны быть вложены в инструменты, а не быть доступными только кому-то одному |
| Необходимость в дорогостоящем обучении персонала технологиям, чтобы сделать работу сотрудников продуктивной | Время обучения уменьшается с включением деталей задания в инструменты EPSS |
| Сокращение персонала, связанного с ИС | Требует минимум помощи от других людей |

### *Сущность и функции EPSS*

Электронные системы поддержки исполнения – это системы поддержки человеческой деятельности, которые могут манипулировать большим количеством информационно связанных задач для предоставления возможностей решения проблем, а также обучающих возможностей для повышения эффективности исполнения заданий людьми, предоставляя информацию и идеи как линейным и нелинейным способом, так и по запросу пользователя.

EPSS основаны на разных сферах применения. Исходя из этого их можно классифицировать по следующим типам:

1) интегрированные с программным обеспечением – предназначены для поддержки ПО;

2) интегрированные с работой – разработаны для задач/работ, основанных на применении компьютера;

3) интегрированные с операциями – предназначены для работы, не связанной с применением компьютера.

Поддержка для исполнения заданий с EPSS обычно предлагается двумя путями. Во-первых, «залатыванием» пробелов в необходимой квалификации, используя обучение «точно в срок» (just-in-time). Во-вторых, давая пользователям гибкий и эффективный доступ к материалам, ориентированным на данную задачу. Исходя из этого, ниже приводятся несколько различных функций, которые EPSS стараются предоставить:

– быстрый доступ к информации, связанной с данной работой;
– необходимое базовое обучение;
– помощь и руководство (пользовательские и системные);
– советы и рекомендации;
– обзоры шагов и процедур работы или задания;
– практический опыт (в смоделированной среде);
– дополнительный мониторинг исполнения и поддержку рекомендациями;
– библиотеку и информационную поддержку.

Можно выделить следующие принципы поддержки исполнения.

1. Установить и сделать приоритетными решающие сферы исполнения в сфере деятельности и затем определить подходящие стратегии для улучшения исполнения.

2. Попытаться разработать механизированные средства и автоматизированные инструменты, чтобы содействовать улучшению в персональном исполнении и в исполнении в организации в целом, признавая проблемно-ориентированный опыт.

3. Определить общие и проблемно-ориентированные инструменты и процессы, которые предоставляют поддержку по ходу работы и улучшают выполнение задачи.

4. Попытаться установить и, если возможно, исключить все информационные помехи и ненужные информационные структуры в организации и непосредственно в рабочей среде.

5. Установить подходящую комбинацию средств массовой информации, мультимедиа, Интернет и телекоммуникаций для оптимизации информационных потоков и межперсональных связей.



6. Когда пользователь или работник имеет установленный недостаток опыта, постараться поправить эту ситуацию, используя обучение «точно вовремя» и обучающие технологии.

7. Всегда, когда это выполнимо, система поддержки исполнения должна индивидуально подстраивать стили обучения и, таким образом, стараться максимизировать ее полезность для широкого круга пользователей и ситуаций исполнения задач.

8. Определить соответствующие группы людей, обладающих опытом решения требуемых проблем, и предоставить инфраструктуру, необходимую для облегчения коллективной работы.

9. Всегда, когда это выполнимо, пытаться использовать знающих агентов со средствами EPSS, чтобы определить, какой опыт необходим для решения данной задачи, найти источники этого организационного опыта относительно данной задачи и улучшить компоненты ПО.

10. Попытаться предоставить средства для создания корпоративного фонда знаний и опыта, с помощью которых можно поддержать или улучшить уровень исполнения [6].

### *Компоненты EPSS*

Системы поддержки исполнения обычно используют графический пользовательский интерфейс и включают в себя следующие типичные компоненты (табл. 2).

Таблица 2

**Компоненты EPSS**

| Инструменты | Информационная база | Консультант | Знания |
|---|---|---|---|
| Текстовый процессор, электронные таблицы, базы данных | On-line документы, соответствующие материалы | Советы экспертов | Мультимедийное компьютерное обучение |
| Шаблоны и формы | Информационные базы данных, «исторические» данные по различным ситуациям | Контекстная on-line помощь | Смоделированные ситуации и сценарии |

Инструменты – производительное ПО (текстовые редакторы, электронные таблицы и т. д.), используемое с формами и шаблонами.

Информационная база – тематическая on-line информация (часто называется «infobase»), гипертекстовые on-line средства помощи, статистические базы данных, мультимедийные базы данных и базы накопленных данных по различным ситуациям.

Консультант – интерактивная рассуждающая экспертная система, основанная на данных по ситуациям, или тренирующее средство, которое проводит пользователя через процедуры исполнения и принятия решений.

Знания и опыт – обучение, основанное на компьютере, такое как интерактивные учебные пособия, мультимедиа-обучение, использующее моделирование ситуаций и сценариев [3].

### *Применение электронных систем поддержки исполнения на предприятиях*

В настоящее время существует тенденция преобразования электронной поддержки исполнения из индивидуальных форм в организационные. Такие модели можно назвать организационными системами поддержки исполнения (Organizational Performance Support System – OPSS). Основным компонентом OPSS является база знаний.

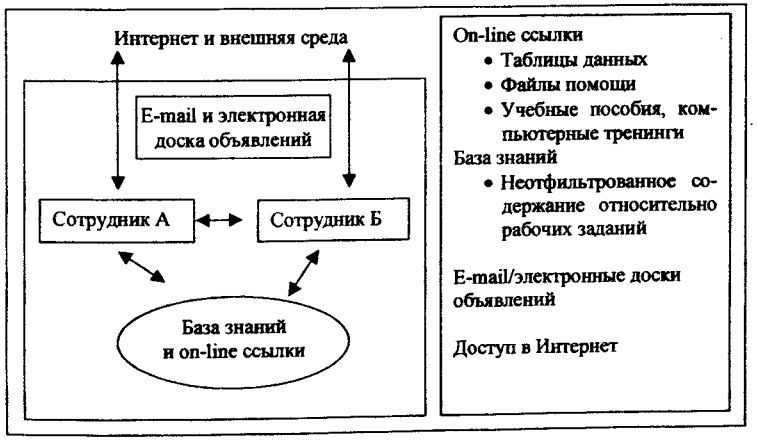
На рисунке показаны потоки информации в такой OPSS. Ввод и обратная связь замыкают все группы в обучающей системе с другими и с базой знаний.

Компоненты OPSS состоят из:

– on-line ссылок на
  а) таблицы данных;
  б) файл помощи;
  в) учебные пособия;
  г) заархивированные электронные обсуждения;
– базы знаний;
– электронной почты;
– доступа в Интернет.

В этой модели доступ к информации и связь не ограничены и снабжены поддержкой. Работники «достают» из базы знаний чужой внешний опыт, чтобы получить информацию для выполнения рабочих заданий. В этом процессе они также пополняют базу знаний своим опытом, таким образом увеличивая объем знаний своей организации. Знания создаются работниками сообща или индивидуально. Организация не может создать знания без участия конкретных сотрудников. В этом и заключается ответственность организации за предоставление среды, благоприятной для создания базы знаний.






Потоки информации в OPPS

Через использование электронных коммуникаций работники могут подтверждать, расширять и обновлять знания организации, изучая внешнюю среду и собирая знания, существующие внутри организации. Организация и ее сотрудники должны рассматривать каждого человека, ситуацию, объект и другие организации как потенциальный ресурс знаний.

Знания должны собираться в организованной форме так, чтобы позже они могли бы быть модифицированы и доступны работникам с целью выполнения рабочих задач. Через использование баз знаний опыт организации может быть сохранен и расширен, предоставляя, таким образом, каждому сотруднику богатый информационный ресурс.

Интерфейс EPSS должен быть дружественным и «понятливым», чтобы увеличить его использование работниками как инструмента работы. В дополнение сотрудникам необходимо дать время, чтобы освоить новое средство, а также получить необходимые навыки для связи с ресурсами информации. Самый важный элемент в EPSS – это

то, что информация должна быть не ограничена и легко доступна всем людям в рамках организации, чтобы поддерживать открытую обучающую систему [2].

**Литература**


1. *Gery G.* Electronic Performance Support Systems. Gery Assoc, 1991.
2. *Bill D. T.* Transforming EPSS to Support Organizational Learning: www.centurionsys.com
3. *Leighton Ch.* What is an EPSS?: it2.coe.uga.edu
4. www.pcd-innovations.com
5. www.leewood.com
6. www.epssworld.com


УДК 378.001.65

© Ю. М. Порховник, М. И. Поляков

Санкт-Петербургский государственный инженерно-экономический университет

## МОДЕЛИ ОПТИМАЛЬНОГО ВЫБОРА ТРАЕКТОРИИ ОТКРЫТОГО ОБРАЗОВАНИЯ

Повышение экономического потенциала страны и качества жизни за счет возрастания уровня образованности населения требует использования новой формы образования, которой является открытое образование.

К числу принципов открытого образования относятся следующие.

1. Конкурентоспособность открытых образовательных услуг, проявляющаяся на рынке этих услуг в виде ценовой и неценовой конкуренции образовательных учреждений. Наличие конкурентных условий требует от образовательных учреждений непрерывного повышения качества образовательных услуг и обоснованного подхода к ценообразованию.

2. Свободный выбор пользователем (обучающимся) образовательного учреждения, соответствующего требованиям пользователя к содержанию образовательной программы, качеству предоставляемых образовательных услуг, плате за образовательные услуги, территориальной доступности учебных центров, поддерживающих дистанционную технологию открытого образования, и характеристикам образовательного учреждения.



3. Модульность образовательной программы, предполагающая ее разбиение на отдельные самостоятельные контекстно-взаимосвязанные циклы дисциплин, имеющие завершенный характер.

4. Возможность формирования пользователем индивидуального учебного плана, состоящего из тех циклов дисциплин, которые соответствуют его требованиям.

5. Возможность выбора пользователем траектории открытого образования, предусматривающей прохождение обучения по различным модулям образовательной программы в нескольких образовательных учреждениях.

Перечисленные принципы открытого образования приводят к постановке задачи оптимального выбора траектории открытого образования.

Содержательная постановка этой задачи сводится к следующему.

Пользователь располагает информацией о различном качестве образовательных услуг по циклам дисциплин, различной плате за обучение и рейтингам образовательных учреждений.

В таблице представлены сведения об открытых университетах Великобритании, занимающих лидирующее положение по качеству преподавания определенных циклов дисциплин в области экономики и информационных технологий [1].

**Открытые университеты Великобритании, лидирующие по качеству преподавания циклов дисциплин в области экономики и информационных технологий**

| Наименование цикла дисциплин | Наименование университета | Стоимость обучения, фунты стерлингов в год | Доля трудоустроенных выпускников, % | Доля иностранных студентов, % | Рейтинговое место университета среди 50 университетов |
|---|---|---|---|---|---|
| Экономика | London School of Economics (LSE) | 8 268 | 94 | 28 | 4 |
| | University of Oxford | 6 300–15 400 | 96 | 33 | 2 |
| Бизнес и менеджмент | University of Manchester Institute of Science & Technology (UMIST) | 6 100–8 100 | 97 | 18 | 15 |
| | Lancaster University | 6 290–8 310 | 95 | 23 | 16 |

Окончание

| Наименование цикла дисциплин | Наименование университета | Стоимость обучения, фунты стерлингов в год | Доля трудоустроенных выпускников, % | Доля иностранных студентов, % | Рейтинговое место университета среди 50 университетов |
|---|---|---|---|---|---|
| Социология | University of Essex | 6 130–8 125 | 92 | 13 | 31 |
| | Lancaster University | 6 290–8 310 | 95 | 23 | 16 |
| Статистика | University of Cambridge | 6 306–15 288 | 97 | 10 | 1 |
| Бухгалтерский учет | University of Manchester | 6 350–15 450 | 95 | 7 | 22 |
| Прикладная математика | University of Cambridge | 6 306–15 288 | 97 | 10 | 1 |
| | University of Oxford | 6 300–15 400 | 96 | 33 | 2 |
| Информационные технологии | University of Cambridge | 6 306–15 288 | 97 | 10 | 1 |
| | University of Glasgow | 6 530–16 320 | 94 | 8 | 24 |
| | Imperial College | 8 000–17 320 | 96 | 19 | 3 |
| | University of Oxford | 6 300–15 400 | 96 | 33 | 2 |
| | University of Warwick | 6 500–8 300 | 97 | 30 | 7 |
| | University of York | 6 390–8 520 | 92 | 6 | 5 |

Выбирая набор образовательных учреждений для прохождения всех циклов дисциплин (учебных модулей) образовательной программы, пользователь стремится либо минимизировать плату за образование при заданном уровне качества образовательных услуг, либо максимизировать уровень качества предоставляемых услуг, укладываясь при этом в имеющиеся в его распоряжении денежные средства для оплаты образования.

При выборе образовательных услуг пользователь может выдвигать и ряд других условий: территориальная доступность учебного центра, доля трудоустроенных выпускников, доля иностранных студентов, международное признание диплома, язык преподавания, общий рейтинг образовательного учреждения и т. д.



Можно предложить следующие модели оптимального выбора траектории открытого образования.

*Модель минимизации стоимости образовательных услуг.* Данная модель может быть представлена в виде задачи целочисленного программирования с булевыми (двоичными) переменными.

Пусть $x_{ij} = 1$, если $i$-й модуль образовательной программы пользователь проходит в $j$-м образовательном учреждении, и $x_{ij} = 0$ – в противном случае.

Требуется минимизировать стоимость образовательных услуг,

$$P = \sum_{i \in I} \sum_{j \in J} p_{ij} x_{ij} + \sum_{j \in J} p_j y_j \to \min, \tag{1}$$

при соблюдении ряда ограничений:

$$\sum_{i \in I} \sum_{j \in J} a_i g_{ij} x_{ij} \geq G_{\text{доп}}; \tag{2}$$

$$\sum_{j \in J} b_{kj} y_j > (=, <) B_{\text{доп}\,k}, \ \forall k \in K; \tag{3}$$

$$\sum_{j \in J} x_{ij} = 1, \ \forall i \in I; \tag{4}$$

$$Y_j = \begin{cases} 1, & \text{если} \sum_{i \in I} x_{ij} > 0; \\ 0, & \text{в противном случае;} \end{cases} \tag{5}$$

$$x_{ij} = \{0, 1\}. \tag{6}$$

В модели (1)–(6) приняты следующие обозначения:

$p_{ij}$ – плата за обучение по $i$-му модулю в $j$-м образовательном учреждении;

$I$ – множество модулей, составляющих образовательную программу, выбираемую пользователем;

$J$ – множество образовательных учреждений, предлагающих образовательные услуги по одному, нескольким или всем модулям образовательной программы пользователя;

$g_{ij}$ – оценка качества образовательных услуг по $i$-му модулю в $j$-м образовательном учреждении;

$a_i$ – весовой коэффициент $i$-го модуля в общей оценке качества образовательной программы;

$G_{доп}$ – допустимый уровень качества образовательных услуг по образовательной программе в целом;

$b_{kj}$ – значение $k$-го показателя, характеризующего $i$-е образовательное учреждение в дополнение к качеству образовательных услуг;

$K$ – множество наименований показателей, характеризующих образовательное учреждение помимо качества образовательных услуг (территориальная доступность учебного центра, доля трудоустроенных выпускников, доля иностранных студентов, общий рейтинг образовательного учреждения и т. д.);

$B_{доп\,k}$ – допустимое значение $k$-го показателя;

$p_j$ – первоначальная плата за обучение в $j$-м образовательном учреждении, связанная с организационным обеспечением обучения (оформление пользователя, заполнение базы данных «Информация» и др.). Эта составляющая платы за обучение не зависит от количества учебных модулей, выбранных пользователем в данном вузе;

$y_j$ – двоичная переменная, принимающая значение 1, если $i$-е образовательное учреждение входит в выбранную траекторию образования, и 0 – в противном случае.

Ограничение (4) обеспечивает обязательность прохождения $i$-го учебного модуля, причем в единственном образовательном учреждении.

Наличие слагаемого $\sum_{j\in J} p_j y_j$ в целевой функции (1) отражает некоторые преимущества прохождения всей образовательной программы в одном образовательном учреждении и сдерживает расширение числа используемых образовательных учреждений в решении задачи.

*Модель максимизации уровня качества образовательных услуг.* Данная модель описывает взаимную задачу по отношению к раннее рассмотренной исходной задаче. В этом случае ограничение на уровень качества образовательных услуг становится критерием, а критерий исходной задачи – ограничением.

Таким образом, в данной модели требуется максимизировать уровень качества образовательных услуг,

$$G = \sum_{i\in I}\sum_{j\in J} a_i g_{ij} x_{ij} \to \max, \qquad (7)$$



при соблюдении следующих ограничений:

$$\sum_{i\in I}\sum_{j\in J} p_{ij} x_{ij} + \sum_{j\in J} p_j y_j \le P_{доп}; \qquad (8)$$

$$\sum_{j\in J} b_{kj} y_j > (=,<) B_{доп\,k}, \ \forall k \in K; \qquad (9)$$

$$\sum_{j\in J} x_{ij} = 1, \ \forall i \in I; \qquad (10)$$

$$Y_j = \begin{cases} 1, & \text{если } \sum_{i\in I} x_{ij} > 0; \\ 0, & \text{в противном случае;} \end{cases} \qquad (11)$$

$$x_{ij} = \{0,1\}, \qquad (12)$$

где $P_{доп}$ – допустимая стоимость образовательных услуг.

Выбор оптимальной траектории открытого образования должен основываться только на множестве паретооптимальных предложений образовательных учреждений. Иными словами, увеличение платы за образовательные услуги должно сопровождаться повышением качества этих услуг.

Оценка качества открытых образовательных услуг является сложной самостоятельной задачей. Можно предложить несколько подходов к ее решению:

– экспертная оценка группой независимых специалистов качества информационных образовательных ресурсов, квалификации тьюторов и принятой в данном учреждении технологии дистанционного образования;

– использование теории нечетких множеств;

– использование статистических данных об академической успеваемости пользователей по итогам тестового контроля;

– оценка среднего времени самостоятельной работы пользователей, необходимого для прохождения учебного модуля;

– анализ фактического выбора образовательных учреждений пользователями;

– механизм опросов пользователей системы открытого образования;

– использование косвенных показателей, характеризующих качество услуг образовательного учреждения (рейтинг образовательного учреждения, процент трудоустроенных выпускников и т. д.);

– механизм государственного лицензирования и аккредитации по соответствующей специальности;

– интегрированная оценка, представляющая собой свертку оценок по нескольким подходам.

Очевидно, что обоснованный выбор траектории открытого образования требует наличия соответствующей исходной информации и квалификации лица, принимающего решение. Поэтому, как правило, такой индикативный (рекомендательный) выбор должен осуществляться консалтинговым центром системы открытого образования по заказу пользователя.

В качестве метода решения задачи оптимального выбора траектории открытого образования может быть предложен метод «ветвей и границ» [2].

**Литература**

1. Школы Ее Величества: www.begin.ru

2. *Глухов В. В., Медников М. Д., Коробко С. Б.* Математические методы и модели для менеджмента. СПб.: Изд-во «Лань», 2000.

УДК 378.001.658.011

**© И. И. Рыкова, О. А. Решетова**

Санкт-Петербургский государственный инженерно-экономический университет

## НЕКОТОРЫЕ ПОЛЕЗНЫЕ ПРИЕМЫ РАБОТЫ С МАССИВАМИ В ТУРБО ПАСКАЛЕ

Одним из недостатков языка программирования Турбо Паскаль, за который его часто справедливо критикуют, является невозможность работы с массивами переменной длины. Отчасти выходом из положения является введение так называемых «открытых массивов», т. е. формальных параметров подпрограмм, в которых не указывается размерность массива. Если в описании подпрограммы в качестве формального параметра фигурирует открытый массив, то соответствующим ему фактическим параметром может быть одномерный массив любой длины. Таким образом, одна подпрограмма может обрабатывать массивы различной размерности. Нижняя и верхняя границы массива при обработке его в подпрограмме в этом случае возвращаются функциями Low и High, параметром которых является массив-переменная. К сожалению, в Турбо Паскале возможна работа лишь с одномерными открытыми массивами, двумерных же открытых массивов не существует.

Еще одним хорошо известным способом обработки массивов (одно- и многомерных), длина которых определяется в ходе выполнения программы, является задание в разделе описания типов максимально возможного числа элементов массива. При этом переменная этого типа может иметь любое, меньшее или равное объявленному ранее при объявлении типа, количество элементов. Недостатком этого метода является нерациональное расходование памяти. Поскольку память под статические переменные, как известно, выделяется на этапе компиляции, то под переменную заданного типа память будет выделена по максимуму, а реально использована лишь часть ее.

В том случае, если количество элементов одно- или многомерного массива становится известно лишь в процессе выполнения программы или одна подпрограмма должна обрабатывать массив с разным количеством элементов, можно воспользоваться указателем на массив, а также тем фактом, что в Паскале не всегда ведется строгий контроль за принадлежностью переменной заданному диапазону.

Так, известно, например, что если задан одномерный массив из 10 элементов, принадлежащих диапазону 1...100, то при наличии оператора присваивания $a[11]:=2$ компилятор сообщает об ошибке, но если написать сначала $i:=10$, а затем $a[i+1]:=2$, то сообщения об ошибке не возникает. Точно так же, если в программе есть оператор присваивания $a[i]:=101$, то возникает сообщение об ошибке, но при вводе с клавиатуры значения большего 100, сообщения об ошибке не выдается, хотя в дальнейшем это значение может быть изменено компилятором.

Воспользовавшись этим, можно задать базовый тип массива из одного элемента, а память выделять под нужное количество элементов. Так, например, при обработке массива записей можно поступить следующим образом:

```
Type rec=record
     X,y:real
     End;
```

```
trec=array[1..1] of rec; recptr=^trec;
procedure vvod(var a:recptr;n:integer);
    var i:integer;
    begin
        getmem(a,n*sizeof(rec));
            for i:=1 to n do
            readln( a^[i]);
```

Количество элементов в базовом типе оказывается несущественным, важно лишь, что это массив и обращение к каждому из элементов идет по индексу.

Также можно создать и двумерный массив или матрицу.

```
Type matrix=array[1..1,1..1] of real;
    Var a:^matrix; i,j,n,m:integer;
        Begin
            Readln(n,m);
                Getmem(a,n*m*sizeof(real));
                    For i:=1 to n do
                        For j:=1 to m do read(a^[i,j]);
```

Таким образом, отсутствие строгого контроля за принадлежностью переменой заданному диапазону позволяет обрабатывать массивы в динамической памяти, длина которых определяется в ходе выполнения программы.

УДК 378.001.658.011.56

© Ж. Г. Салимьянова

Санкт-Петербургский государственный
инженерно-экономический университет

## К ВОПРОСУ О САМОКОНТРОЛЕ В УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ

В научных трудах содержатся разные толкования понятия «самообучение». Проблематика самообучения обнаруживается во многих работах, но излагается формально, иногда вместо термина «самообучение» используется термин «самообразование». Очевидно, это связанно с ростом уровня просвещения и с постоянной необходимостью обогащения общего и специального образования независимо от места и положения, занимаемого личностью в обществе.

Известно, что самообразование – это такой вид обучения, цели, содержание, условия и средства которого зависят от самого субъекта.



Оптимального уровня самообразование достигает тогда, когда оно преобразуется в постоянную жизненную потребность человека, основу его образования в течение всей жизни, основу его поведения и образа жизни.

В связи с тем, что высшая школа существенно отличается от средней не только специализацией подготовки, но и большим объемом учебного материала, некоторые студенты не справляются с трудностями в усвоении программного материала, у них формируется чувство неудовлетворенности и негативное отношение к учению в целом. Следовательно, встает задача помочь студентам овладеть научными основами учебной работы в вузе.

Мысль о том, что система организованного обучения должна дать учащимся не только знания того или иного учебного предмета, но и способы эффективного усвоения знаний, не является совершенно новой. Существенно то, что в последние годы в связи с возросшими требованиями подготовки специалистов формирование у студентов умения учиться выступило в качестве важнейшей самостоятельной задачи вузовского обучения.

Опыт подсказывает, что обучение учебной деятельности следует проводить и в специальном курсе, и в пределах конкретных дисциплин. В таком случае важным фактором успеха являются согласованность и единообразие сведений о действиях, которые излагаются студентам как в специальном курсе, так и на занятиях по конкретным дисциплинам. Нельзя забывать, что обучение учению не однократное мероприятие, а постоянно идущая работа в течение всего периода обучения в высшей школе.

Потребность в познании, в познавательной деятельности – одна из главных человеческих потребностей, на основе которой происходит освоение индивидуумом человеческого опыта. Что касается учебно-познавательной деятельности, то она мотивируется познавательными интересами, направленными на научные факты и закономерности, на методы и приемы познания, т. е. на ценность творческого знания.

Синтез собственно познавательных интересов и мотивации достижения личности лежит в основе того, что называют творческой активностью познающего субъекта. Учение наиболее эффективно тогда, когда выделяются на первый план коммуникативные, смысловые его аспекты. Естественно, в обучении коммуникативные процессы

весьма специфичны, тем не менее, они всегда остаются необходимым условием организации учебно-познавательной деятельности личности, занятой образованием и самообразованием.

Основным средством коммуникации знаний является текст. Он может быть выражен в устной или письменной форме. Текст – это функциональная единица, в нем содержится информация об объектах окружающей действительности, но представлена она с определенной целью. В общей форме всякий текст является средством общения между людьми. Существуют три основных условия (критерия), определяющих эффективность воздействия текстов на личность: значимость содержания для личности, т. е. соответствие ее потребностям и интересам; доступность для понимания; убедительность аргументов и выводов.

Работа с учебным текстом – это, прежде всего, анализ его логического содержания. Главное для студентов – понять, какую познавательную задачу ставит автор текста, и какие способы ее разрешения предлагаются в тексте.

Подготовленность студентов к восприятию текста дает им возможность «видеть» проблемы (вопросы, задачи) в различных текстах, даже если проблема не формулируется автором в ясной форме. Замечено, что чем шире привлекаемый материал для раскрытия определенной проблемы (учебный, научно-популярный, специальный, практический), тем больше возможностей не только для глубокого освоения данного материала, но и для формирования обобщенного подхода к самостоятельному анализу текста.

Существуют разнообразные умения самообразовательной работы. С одной стороны, это новейшие достижения компьютерной техники, с другой стороны, умение найти и выбрать необходимую литературу, умение читать книгу, работать над текстом с целью его освоения.

Суммируя взгляды многих исследователей, можно назвать четыре основных метода чтения: чтение – просмотр; выборочное чтение; чтение полное или сплошное, когда прочитывается весь текст, ограничиваясь условными пометками; чтение с проработкой материала, т. е. изучающее чтение с использованием новых форм дистанционного общения с помощью компьютера.

В самостоятельной работе с материалом применяют все перечисленные методы, но в период, когда студент систематически работает над усвоением основ наук, особое значение приобретает последний метод с использованием представляемых услуг глобальными компьютерными информационными сетями.



Как же решается проблема самоконтроля при подготовке специалистов в системе высшего образования?

Прежде всего следует отметить, что процесс развития у студентов оценочно-результативного компонента учебной деятельности идет в направлении от проверки правильности выполнения и оценки этой деятельности (констатирующего самоконтроля) к оценке и анализу процесса его достижения (корректирующему самоконтролю). Важно привить студентам потребность пользоваться системой приемов, правил по проверке и оценке качества усвоения изучаемого материала. Обычно педагоги недооценивают фактор самоконтроля, преувеличивая значение контроля. А между тем не всякая проверка оказывает положительное влияние на достижения студентов.

Воспитательное значение оценка как результат проверки имеет тогда, когда является правильной, по убеждению преподавателя, справедливой, по убеждению студентов, отвечающей общественно принятым критериям оценок. Студенты отмечают, что проверка и оценка знаний преподавателем заставляет их лучше готовиться к занятиям, искать и использовать более эффективные способы усвоения изучаемого материала, к числу которых они относят и самоконтроль.

Улучшению контроля за учебной работой студентов способствует также использование на практических занятиях и такой его формы, как взаимоконтроль. Эффективность взаимного контроля как стимула формирования самоконтроля подтверждается применением его на лабораторных занятиях по изучению офисных пакетов прикладных программ. При включении студентов в оценочную деятельность существенное значение придается усвоению ими образцов, по которым они могут сравнивать полученные результаты. Смысл учения в том, что новое для студента содержание должно быть связано с ранее приобретенным, должно расширять объем познавательных структур.

Студенты с большим вниманием и заинтересованностью воспринимают рекомендации. Более того, анализируя конкретные образцы учебного труда, они отчетливо начинают понимать сущность приемов самопроверки, перестраивают свою учебную работу так, чтобы в процессе подготовки к занятиям использовать самоконтроль.

Вначале студенты планируют последовательность выполнения того или иного задания, сопоставляют и оценивают известные им способы учебной работы, продумывают, возможные результаты их применения и лишь после этого начинают выполнять задание.

Наблюдения показывают, что систематическая работа, направленная на овладение приемами самокоррекции, изменяет стиль учебной деятельности и дает положительные результаты.

УДК 378.001.658.011.56

© В. В. Тарзанов

Санкт-Петербургский
институт гостеприимства

## БУДУЩЕЕ ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ: СТРУКТУРНЫЙ ИЛИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД?

Развитие объектно-ориентрованной технологии программирования, начавшееся с середины 1980-х гг., к настоящему времени достигло той поры зрелости, когда приходится говорить о начале «революции в программировании». Безусловно, это не могло не затронуть взглядов на жизненный цикл и, в частности, на содержание проектирования прикладных информационных систем, важнейшую часть которых составляет программное обеспечение.

Сущность структурного подхода к разработке информационных систем (ИС) заключается в ее декомпозиции (разбиении) на автоматизируемые функции: система разбивается на функциональные подсистемы, которые в свою очередь делятся на подфункции, подразделяемые на задачи и т. д. Процесс разбиения продолжается вплоть до конкретных процедур. При этом автоматизируемая система сохраняет целостное представление, в котором все составляющие компоненты взаимоувязаны. При разработке системы «снизу вверх» от отдельных задач ко всей системе целостность теряется, возникают проблемы при информационной стыковке отдельных компонентов.

Все наиболее распространенные методологии структурного подхода базируются на ряде общих принципов. В качестве двух базовых принципов используются следующие:



– принцип «разделяй и властвуй» – принцип решения сложных проблем путем их разбиения на множество меньших независимых задач, легких для понимания и решения;

– принцип иерархического упорядочивания – принцип организации составных частей проблемы в иерархические древовидные структуры с добавлением новых деталей на каждом уровне.

Выделение двух базовых принципов не означает, что остальные принципы являются второстепенными, поскольку игнорирование любого из них может привести к непредсказуемым последствиям (в том числе и к провалу всего проекта). Основными из этих принципов являются:

– принцип абстрагирования – заключается в выделении существенных аспектов системы и отвлечения от несущественных;

– принцип формализации – заключается в необходимости строгого методического подхода к решению проблемы;

– принцип непротиворечивости – заключается в обоснованности и согласованности элементов;

– принцип структурирования данных – заключается в том, что данные должны быть структурированы и иерархически организованы.

В структурном анализе при проектировании ИС используются в основном две группы CASE-средств: средства, описывающие функции, выполняемые системой, и средства, формализующие отношения между данными.

В основе первых лежат методологии функционально-структурного анализа (например, SADT, ее подмножество IDEF0, IDEF3 и т. д.). При этом для объекта предметной области строится его иерархическая функциональная модель, отображающая производимые им действия и связи между этими действиями. Вторая группа ориентирована на проектирование баз данных (БД), основываясь на семантическом моделировании и генерации реляционных схем БД.

В наиболее общей и классической постановке объектно-ориентированный подход базируется на следующих концепциях:

– классов;

– иерархии и наследования классов;

– объекта и идентификатора объекта;

– атрибутов и методов.

Наиболее важным новым качеством БД, которого позволяет достичь объектно-ориентированный подход, является поведенческий

аспект объектов. В прикладных информационных системах, основывающихся на БД с традиционной организацией (вплоть до тех, которые базировались на семантических моделях данных), существует принципиальный разрыв между структурной и поведенческой частями. Структурная часть системы поддерживается всем аппаратом БД, ее можно моделировать, верифицировать и т. д., а поведенческая часть создается изолированно. В частности, отсутствует формальный аппарат и системная поддержка совместного моделирования и гарантирования согласованности этих, структурной (статической) и поведенческой (динамической), частей. В среде объектно-ориентированных баз данных (ООБД) проектирование, разработка и сопровождение прикладной системы становится процессом, в котором интегрируются структурный и поведенческий аспекты. Очевидно, что для этого нужны специальные языки, позволяющие определять объекты и создавать на их основе прикладную систему.

Основные трудности объектно-ориентированного моделирования данных заключаются в том, что такого развитого математического аппарата, на который могла бы опираться общая объектно-ориентированная модель данных, пока не существует. В большой степени поэтому до сих пор нет базовой объектно-ориентированной модели.

Как отмечают многие исследователи и разработчики, объектно-ориентированная система БД представляет собой объединение системы программирования и СУБД (альтернативная, но не более проясняющая суть дела точка зрения состоит в том, что объектно-ориентированная СУБД – это СУБД, основанная на объектно-ориентированной модели данных).

В среде ООБД должны отсутствовать противоречия между структурной и поведенческой частями проекта, а также поддерживаться эффективное управление сложными структурами данных во внешней памяти. В отличие от случая реляционных систем, где при создании приложения приходится одновременно использовать ориентированный на работу со скалярными значениями процедурный язык программирования и ориентированный на работу с множествами декларативный язык запросов (это принято называть потерей соответствия – impedance mismatch), языковая среда ООБД – это объектно-ориентированная система программирования, естественно включающая средства работы с долговременными объектами. «Естественность» включения средств работы с БД в язык программирования означает, что работа с долговременными (хранимыми во внешней БД) объектами должна происходить на основе тех же синтаксических конструкций (и с той же семантикой), что и работа с временными, существующими только во время работы программы, объектами.



Эта сторона ООБД наиболее близка родственному направлению языков программирования баз данных. Языки программирования ООБД и БД во многих своих чертах различаются только терминологически. Существенным отличием является лишь поддержание в первых подхода к наследованию классов. Кроме того, языки БД, как правило, более развиты как в отношении системы типов, так и в отношении управляющих конструкций.

Другим аспектом языкового окружения ООБД является потребность в языках запросов, которые можно было бы использовать в интерактивном режиме. Если доступ к объектам внешней БД в языках программирования ООБД носит в основном навигационный характер, то для языков запросов более удобен декларативный стиль. Декларативные языки запросов к ООБД менее развиты, чем языки программирования ООБД, и при их реализации возникают существенные проблемы.

Естественным подходом к построению языка программирования ООБД было бы использование (с необходимыми расширениями) некоторого существующего объектно-ориентированного языка.

Потребность в поддержании в объектно-ориентированной СУБД не только языка (или семейства языков) программирования ООБД, но и развитого языка запросов в настоящее время осознается практически всеми разработчиками. Система должна поддерживать легко осваиваемый интерфейс, прямо доступный конечному пользователю в интерактивном режиме.

При выборе языка ООБД на основе ненавигационных языков запросов возможно существование двух подходов.

Первый подход – языки, являющиеся объектно-ориентированными расширениями языков запросов реляционных систем. Наиболее распространены языки с синтаксисом, близким к известному языку SQL. Это связано, конечно, с общим признанием и чрезвычайно широким распространением этого языка.

Второй подход основывается на построении полного логического объектно-ориентированного исчисления. По поводу построения

такого исчисления имеются теоретические работы, но законченный и практически реализованный язык запросов пока неизвестен.

Таким образом, если будущее за объектно-ориентированным подходом к проектированию ИС, то это все-таки отдаленное будущее. И не только потому, что в настоящее время отсутствуют глубокий методический аппарат ООБД и язык запросов. Это дело времени. Зададим себе вопросы: возможным было бы появление объектно-ориентированного программирования вообще в отсутствие структурного? И не включает ли в себя объектно-ориентированный подход все компоненты структурного? Ответы не кажутся столь очевидными. Однако вспомним, сколько времени должно было пройти, сколько версий языков высокого уровня сменило друг друга, пока в мир программирования не пришла идея объединить в одной структуре данные и методы их обработки. Относительно последних следует отметить, что это самые обыкновенные подпрограммы (процедуры), которые должны строиться по всем правилам структурного программирования.

Кроме того, сама эволюция развития CASE-средств как основных инструментов разработки ИС говорит о том, что рано (или даже нельзя) отказываться от структурного подхода.

Не так давно известная фирма «Rational Software Corporation», продукты которой реализуют объектно-ориентированный подход к проектированию ИС, выпустила собственное средство моделирования данных Data Modeler, которое стало доступно разработчикам, использующим в своей работе Rational Rose Professional Modeler Edition. Заметим, что в ранних версиях Rational Rose возможно было строить объектную модель, но нельзя было построить модель данных или системный каталог сервера БД.

При использовании Data Modeler:

– поддерживается большинство возможностей структурных CASE-средств в плане физического моделирования данных;

– обеспечивается генерация физической структуры БД;

– реализуется концептуальное соответствие модели данных и объектной модели;

– обеспечивается тесная интеграция с Rational Rose, а диаграмма Data Model естественным образом вписывается в общую объектно-ориентированную технологию разработки ИС.

Относительно компонента Data Model следует отметить, что это самая «структурная» часть Data Modeler, поскольку именно она предоставляет возможности по созданию и редактированию таблиц и их элементов (включая ограничения, триггеры и т. д.), а также связей между ними. Иными словами, в Data Model реализованы все возможности структурных CASE-средств вплоть до генерации физической схемы БД. Единственное, что в нем не реализовано (и, по-видимому, никогда не будет реализовано), – это функция проверки корректности логической структуры БД, обеспечивающей целостность, непротиворечивость и полноту данных, а также отсутствие различного рода аномалий. Поэтому Data Modeler сгенерирует физическую схему БД и соответствующую объектную модель со всеми теми ошибками, которые были допущены при проектировании логической структуры системы.

Безусловно, ни одно из структурных CASE-средств также не реализует этой функции в полном объеме. Но ведь ни одно структурное CASE-средство никогда и не претендовало на истину в последней инстанции.

Следовательно, этап структурного анализа обязан присутствовать при проектировании ИС (кстати, на этом основывается любая модель жизненного цикла ИС, которая в качестве первого этапа включает системный анализ предметной области при помощи структуризации и абстрагирования).

Подводя итог, отметим, что будущее проектирования ИС, видимо, в рациональном сочетании, синтезе структурного и объектно-ориентированного подходов, в умелом совместном использовании сильных сторон этих казалось бы антагонистических направлений. Истина, как отмечал Рене Декарт, всегда располагается где-то посередине. Важно только правильно определить это «где-то».

УДК 378.001.658.011.56

**© А. Е. Фарафонов**

ООО «Берег», Санкт-Петербург

## ЭКОНОМИКО-МАТЕМАТИЧЕСКОЕ, ИНФОРМАЦИОННОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ РЕШЕНИЯ ЗАДАЧИ УПРАВЛЕНИЯ ЗАПАСАМИ

Управление запасами – это создание и гарантированный контроль состояния комплекса запасов по всем этапам логистической цепи товара при минимальных издержках, соответствующих уровню

активности предприятия. Под логистической цепью понимается путь, по которому проходят материальный поток, финансовый поток и отражающий их движение информационный поток от поставщика до потребителя готовой продукции.

Решение задачи управления запасами является необходимым условием ведения практически любого вида бизнеса – будь то производство любого масштаба и направления или торговля от розницы до крупного опта. Даже при высоком уровне организации оперативных процессов возможны ситуации, при которых ритмы поставок и потребления могут не совпадать. Помимо этого, под воздействием различных внутренних и внешних факторов могут увеличиваться издержки на поддержание товарного (или ресурсного) запаса. Поэтому вся система управления запасами должна быть не только тщательно выстроена и сбалансирована, кроме того, данная система должна постоянно анализироваться, гибко и оперативно перестраиваться при изменяющихся условиях рынка и возрастающих либо уменьшающихся потребностях.

Рассмотрим проблему решения задачи управления запасами, способы и пути ее решения на примере крупной оптовой торговой компании. Решение задачи управления запасами в этом случае имеет ряд особенностей. К ним относятся:

– широкая сеть поставщиков; при этом необходимо учитывать, что различные виды товаров имеют свои отличные сроки изготовления и поставки;

– обширная номенклатура – до 10 000 позиций;

– необходимость поддержания широкого ассортимента товаров;

– наличие сезонных колебаний объема продаж как в общем по всему ассортименту, так и с учетом сезонных колебаний объема продаж отдельных видов продукции, отличающихся по срокам и продолжительности от общих колебаний;

– наличие в ассортименте продукции или видов продукции с различными объемами продаж, различной скоростью реализации, различной оборачиваемостью, наконец, различной наценкой;

– фактор конкурентной борьбы.

Все эти факторы делают задачу управления запасами на данном уровне нетривиальной, требующей серьезного подхода. Возникает необходимость построения экономико-математической модели, которая позволила бы учитывать все многообразие внутренних и внешних, временных и перманентных факторов, влияющих на структуру



товарного запаса. Построение данной модели позволит пошагово решать следующие задачи:

– оптимизация структуры товарного запаса;

– оптимизация движения финансовых потоков;

– повышение эффективности финансовых вложений в товарный запас.

Поскольку в качестве примера мы взяли крупную компанию с широким ассортиментом, большим количеством поставщиков и покупателей, объемы информации, описывающие бизнес-процессы не могут быть обработаны без построения информационной системы. Таким образом, необходимо построить информационную систему, реализующую несколько этапов. Первый этап – анализ накопленных статистических данных и подготовка исходных данных для построенной экономико-математической модели. Следующий этап информационной системы – воплощение построенной экономико-математической модели. И, наконец, на завершающем этапе – результаты работы экономико-математической модели представляются в виде, облегчающем анализ статистических данных; позволяющем прогнозировать варианты развития ситуации, варьируя входные параметры; помогающем в принятии решения.

Рассмотрим более подробно структуру товарного запаса. Весь товарный запас можно подразделить на следующие группы и подгруппы:

– основной:
  рабочий;
  страховой;
– временный:
  сезонный;
  маркетинговый;
  конъюнктурный;
– вынужденный:
  неликвиды;
  брак.

Рабочий товарный запас – запас, который расходуется и пополняется более-менее равномерно. Его объем и темпы расхода и пополнения легко прогнозируются на основе статистических данных. Страховой же запас служит для сглаживания различного рода возмущений. Он должен обеспечить бесперебойное снабжение клиентов

в случае неравномерного производства у поставщика, незапланированного роста сбыта, задержки доставки товара.

Как уже отмечалось ранее, различные виды или группы видов товара характеризуются разной долей влияния на конечный результат (прибыль, оборот и т. д.). Соответственно, значение поддержания в товарном запасе определенного количества тех или иных видов товара (позиций ассортимента) также колеблется.

Чтобы оценить вклад в общий результат различных видов товара, существует довольно простой и действенный механизм – ABC (XYZ)-анализ и правило Парето. В основном в логистике ABC-анализ используется для сокращения количества товарного запаса, высвобождения «замороженных» средств, уменьшения складских операций с товаром, общего увеличения прибыли и т. п.

Идея ABC-анализа состоит в том, чтобы из всего множества однотипных объектов (позиций ассортимента, например) выделить наиболее значимые с точки зрения обозначенной цели. Таких объектов, как показывает практика, немного, и именно на них необходимо сосредоточить основные усилия. В экономике широко известно так называемое правило Парето, согласно которому лишь 20% объектов приносит 80% результата, и, соответственно, остальные 80% объектов приносят всего лишь 20% результата. Таким образом, чтобы оценить значимость отдельных элементов товарного запаса (ТЗ), необходимо оценить значимость каждого объекта с помощью ABC-анализа и, применив правило Парето, выделить группу *A* (80% вклада), группу *B* (15% вклада) и группу *C* (5% вклада). XYZ-анализ применяется на завершающей стадии и служит для оценки доли возмущений (всплесков, провалов) в расходовании ТЗ.

Таким образом, проведя подобный анализ, имея статистику расходования ТЗ за довольно продолжительный промежуток времени, можно прогнозировать расход товара на перспективу и рассчитывать объем основного и страхового товарного запаса. Следующий фактор, который необходимо учесть, – это интервалы и размеры поставок. Существует множество различных подходов в пополнении запасов равными объемами через неравные промежутки времени, неравными объемами через равные промежутки времени и т. д. В случае значительных колебаний объемов и интервалов поставок расчет объема товарного запаса можно произвести по средней арифметической взвешенной:



$$t = \sum t_i \frac{Q_i}{\sum Q_i},$$

где $t_i$ – значение интервалов поставки, дн.;

$Q_i$ – фактический объем поставки с интервалом $t_i$.

Текущий запас в днях потребности можно рассчитать как

$$t = \frac{Q}{q},$$

где $q$ – среднесуточная потребность;

$Q$ – средняя величина партии поставки.

Однако данный метод учитывает только один из четырех факторов, влияющих на объем ТЗ, – интервал (или объем) поставки. Таким образом, требуется построение модели, учитывающей все многообразие факторов, влияющих на размер и структуру ТЗ.

Существует множество научных работ, посвященных обзору действующих экономико-математических моделей решения задачи управления запасами. Их анализ показывает, что при всем своем многообразии все они могут быть сведены к одному или нескольким из перечисленных ниже вариантов:

– политика фиксированного размера запаса (точка заказа и размер заказа – величины постоянные);

– политика регулярного пополнения запасов при фиксированном размере заказа (точка заказа – переменная при постоянном размере заказа);

– политика двух уровней (точка заказа – величина постоянная при переменном размере заказа);

– политика постоянного уровня запасов (размер заказа и точка заказа – величины переменные).

Многообразие существующих экономико-математических моделей подтверждает тот факт, что не существует «единой» задачи управления запасами и общей теории управления запасами.

При построении модели управления запасами следует определить критерии выбора стратегии функционирования. Обычно такими критериями являются максимизация возможной прибыли при минимизации возможных издержек. Необходимо также учесть составляющие издержек, период времени, на котором они действуют, и методы учета факторов случайностей, влияющих на условия задачи. Для определения оптимальной стратегии функционирования необходимо учитывать только те издержки, которые зависят от ее выбора, т. е. переменные издержки.

Таким образом, мы рассмотрели наиболее важные факторы, влияющие на решение задачи управления товарным запасом; факторы, влияние которых необходимо учитывать при построении экономико-математической модели решения задачи управления запасами; причины, по которым, построение экономико-математической модели и основанной на ней информационной системы является необходимым условием решения поставленной задачи для обеспечения бизнес-процессов компании, выбранной нами в качестве примера.

УДК 378.001.658.011.56

**© Г. М. Чернокнижный,**
**С. Б. Чернокнижный**

Санкт-Петербургский государственный
инженерно-экономический университет

## ПОДХОД К СОЗДАНИЮ БАЗЫ ДАННЫХ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ГАЛЬВАНИЧЕСКОГО ПРОИЗВОДСТВА

Системы автоматизированного проектирования технологических процессов (САПР ТП) всегда являлись серьезным инструментом в ускорении технологической подготовки производства и, как следствие, в сокращении сроков освоения новых изделий. Особенно актуальным применение САПР ТП становится в современных условиях наметившейся тенденции промышленного роста в машино- и приборостроении.

Развитие САПР ТП должно идти в двух направлениях: во-первых, в совершенствовании возможностей собственно проектирования технологических процессов (расширение функциональных возможностей системы, совершенствование интерфейса взаимодействия с технологом-проектировщиком, создание элементов искусственного интеллекта и т. п.); во-вторых, в интеграции со смежными производственными и технологическими переделами.

Не вдаваясь в детали второго направления, отметим только, что оно может быть эффективно реализовано с использованием современных сетевых технологий.



Повышение производительности труда технологов и нормировщиков и повышение качества проектных работ должно обеспечиваться, главным образом, за счет работ поискового и расчетного характера, работ по оформлению технических документов, ведения архива техпроцессов.

Это может быть выполнено за счет рационального построения и ведения информационной базы данных.

База данных САПР ТП гальванического производства должна содержать следующие разделы:

– проектирование;
– нормирование;
– техпроцессы;
– служебный;
– номенклатура.

Раздел «Проектирование» должен содержать сведения о производственной системе, используемые для реализации функций проектирования типовых и единичных технологических процессов (ТТП и ЕТП), расчета норм расходов материалов на ТТП.

Раздел «Нормирование» должен содержать данные по нормированию ЕТП, стандартизированные нормативы времени и дополнительные данные, позволяющие провести уточненную идентификацию по каждой операции ЕТП.

Раздел «Техпроцессы» должен содержать все техпроцессы (ТТП и ЕТП) как введенные при первоначальном формировании базы, так и сформированные в результате эксплуатации.

Служебный раздел должен содержать вспомогательную информацию для выполнения системой своих функций (формы документов, необходимую нормативную аргументацию, сообщения об изменениях, приказы и распоряжения, касающиеся гальванического производства и т. п.).

Раздел «Номенклатура» должен содержать базу деталей, обрабатываемых на гальваническом производстве, с указанием их площадей поверхности, типов приспособлений, на которых производится обработка, и емкости каждого приспособления.

САПР ТП, используя механизм управления базой данных, должен обеспечивать:

– расчет площади покрываемой поверхности;
– расчет количества приспособлений, одновременно загружаемых в гальваническую ванну, каждого типа (единичная загрузка);

– формирование и ведение нормативно-справочной информации;
– корректировка ТП;
– проектирование ТТП;
– проектирование ЕТП;
– расчет норм расхода материалов;
– получение справок по базе данных и архиву ТП;
– печать технологической документации.

Очевидно, что работа пользователей САПР ТП может проводиться в режиме разделения времени со многих терминалов:
– отдел главного технолога или металлурга;
– технологическое бюро цеха гальванохимических покрытий;
– цеховая химическая лаборатория;
– центральная заводская лаборатория.

Такая распределенная САПР ТП представляет собой вычислительную систему, построенную на основе реляционной базы данных. Несмотря на наличие разных способов организации в виде баз данных, реляционные СУБД считаются одними из наиболее эффективных. В реляционной базе информация представляется в виде таблиц, а для эффективной организации данных используется теория множеств. В таблицах хранится информация об объектах одного типа. Связанные данные сгруппированы в единую структуру – запись, причем между этими структурами можно определить связи. Такая структура хранения данных позволяет различным образом считывать подмножества связанных записей, хранимых в различных таблицах.

Распределенные вычисления – основа современных вычислительных систем. Они позволяют максимально приблизить данные и вычислительные ресурсы к их потребителям. За счет этого можно уменьшить время реакции вычислительной системы на запрос пользователей, а некоторые элементы сделать полностью автономными. САПР ТП на основе баз данных мощнее, чем просто файлы, так как данные в них лучше структурированы. В эффективно организованной базе отсутствуют дублированные данные, которые пользователю приходится обновлять одновременно.

По принципам организации ядра рассматриваемая САПР ТП относится к группе Database Driven System (DDS) и объединяет системы, сохраняющие информацию проекта в централизованном (едином) хранилище базы данных. Сохранение проекта в базе данных



обеспечивает контроль и управляемость всеми данными проектируемого техпроцесса. Когда наиболее трудоемкая работа – управление данными – переложена с САПР-платформы на СУБД, происходит рациональное перераспределение задач.

САПР-платформа (АРМ технолога-проектировщика) выполняет свои «родные» операции управления: интерфейс для ввода и отображения информации, ввод, оформление проектной документации и т. д.

СУБД (как правило, применяется Microsoft SQL Server или Oracle) занимается своей работой: исполняет запросы к данным, классифицирует и упорядочивает данные, гарантированно сохраняет технологические характеристики и связи между данными, организует коллективную работу над единым проектом и обеспечивает все возможности механизмов СУБД.

Получившая большую популярность СУБД Microsoft SQL Server 2000 работает с другими программными продуктами, образуя стабильное и безопасное хранилище информации для Интернета и интрасетей. В частности, работает с механизмами безопасности и шифрования Windows 2000 Server и поддерживает идентификацию Windows. Это позволяет применять в качестве учетных записей SQL Server 2000 пользовательские и доменные учетные записи Windows 2000. СУБД SQL Server 2000 поддерживает функции динамической самонастройки, таким образом можно не нагружать пользователей решением административных задач. База данных Microsoft SQL Server 2000 позволяет также восстанавливать данные после аварии системы, переводя их в согласованное состояние, зафиксированное до сбоя.

Кроме того, Microsoft SQL Server 2000 прекрасно интегрирована с Microsoft Office, имеет значительные усовершенствования в выполнении трансакций, оперативном резервировании и тиражировании, а также новшества в области автонастройки и автоматического выбора конфигурации.

САПР ТП должна предоставлять конечным пользователям удобный инструмент для ввода, просмотра и анализа данных, вывода на печать необходимой информации. Разработка удобного интуитивно понятного интерфейса пользователя является важной частью построения автоматизированной системы. Среда разработки приложений Visual Basic 6.5 предоставляет широкие возможности доступа и обработки баз данных.

При создании приложения на основе системы управления базами данных Microsoft SQL Server 2000 рационально использовать технологию ADO (ActiveX Data Objects), которая входит в состав программной среды Visual Basic, начиная с версии 5.0. Технология ADO представляет собой модель объектов для доступа как к локальным базам данных на одном компьютере, так и к базам данных клиент-сервер, а также предоставляет возможность для доступа к информации через Интернет. Технология ADO фирмы Microsoft представляет собой объектно-ориентированный интерфейс для новой технологии доступа к данным OLE DB и является частью идеологии универсального доступа к данным Universal Data Access. Это позволяет унифицировать все источники данных.

На рисунке представлена схема доступа к данным на основе технологии ADO. Используемый здесь термин «провайдер данных» можно рассматривать как синоним понятия «драйвер».

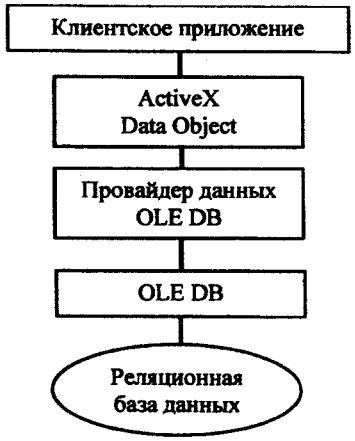



Схема доступа к данным

Технологии ADO значительно упрощают процесс организации совместного доступа и разработку приложений обработки баз данных для работы в локальных и глобальных сетях предприятия.

В соответствии с рассмотренными выше принципами создания функциональной структуры базы данных САПР ТП гальванического



производства и преимуществами СУБД Microsoft SQL Server 2000 и технологии ADO для обработки баз данных применение этой системы имеет все основания.

УДК 378.001.65

© М. А. Шапченко
Санкт-Петербургский государственный
инженерно-экономический университет

## ОРГАНИЗАЦИЯ ХРАНЕНИЯ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ НОВЫХ ТЕХНОЛОГИЙ

Неуклонное увеличение объема данных, обрушивающихся на пользователей компьютерных систем, заставляет исследователей находить новые резервы в уже существующих технологиях и заниматься поиском альтернативных решений. Одним из перспективных направлений в этой области является освоение нанотехнологий.

Пожалуй, наиболее острой проблемой, с которой сталкиваются разработчики устройств хранения данных, становится необходимость увеличения удельной емкости накопителей. А это, в свою очередь, требует уменьшения размеров «ячеек», в которых хранятся отдельные структурные единицы информации.

Если говорить об используемых ныне технологических решениях, то сегодня в тройку наиболее популярных накопителей входят жесткие магнитные диски, оптические диски и носители на базе флэш-памяти. Каждая из этих технологий пока еще имеет резервы для дальнейшего развития, однако рано или поздно наступит момент, когда все потенциальные возможности будут исчерпаны. И тогда возникают принципиально иные решения, прототипы которых пока еще не покинули стен исследовательских лабораторий.

11 июня 2002 г. сотрудники расположенного в г. Цюрихе исследовательского центра компании «IBM» продемонстрировали работоспособный прототип устройства хранения данных, обеспечивающего плотность записи в 1 трлн бит на квадратный дюйм, что на порядок превосходит наилучшие показатели технологий, использующих магнитную запись. Для наглядности можно сказать, что разработанная учеными «IBM» технология позволяет сохранить 25 млн страниц текста на носителе размером с почтовую марку. Столь выдающиеся

результаты стали возможными благодаря исследованиям, проведенным специалистами «IBM» в рамках проекта под кодовым названием «Millipede».

В накопителе Millipede используется принцип механической записи: микроскопические иглы продавливают углубления на поверхности тонкой пластиковой пленки, при этом каждое из таких углублений соответствует одному биту записываемой информации. Это напоминает один из старейших цифровых носителей – перфокарту.

Однако эта «перфокарта» не совсем обычная: во-первых, в Millipede предусмотрена возможность многократной перезаписи, а во-вторых, на площади, эквивалентной одному отверстию классической перфокарты (которое соответствует одному биту), носитель Millipede позволяет уместить более 3 млрд бит информации.

Ядром Millipede является двумерный массив микроприводов, представляющих собой V-образные силиконовые рычаги длиной 70 мкм и толщиной всего 0,5 мкм.

На конце подвеса каждого микропривода имеется обращенная вниз игла длиной чуть менее 2 мкм. Существующая сегодня экспериментальная установка оснащена массивом из 1 024 микроприводов (32 ряда по 32 элемента), физический размер которых составляет 3 на 3 мм.

Специально разработанная конструкция подвеса массива игл выполняет две основные функции: обеспечивает точность позиционирования массива и предохраняет носитель информации от повреждений, компенсируя внешние физические воздействия (вибрации и удары). Управляющая электронная схема, аналогичная используемой в чипах DRAM-памяти, позволяет одновременно посылать индивидуальные команды каждому из микроприводов, обеспечивая их слаженную совместную работу. Каждая игла обслуживает область размером 100 на 100 мкм; точное перемещение носителя информации в двух направлениях осуществляет прецизионный электромагнитный привод. Благодаря малому ходу носителя энергопотребление системы невелико.

Все необходимые операции: чтение, запись, стирание и перезапись – осуществляются при соприкосновении игл с тонкой полимерной пленкой, покрытой слоем силиконового материала толщиной всего несколько нанометров. Нанесение углубления, соответствующего одному биту, производится путем нагревания встроенного в



микропривод резистора до 400°С. Нагретая до этой температуры игла размягчает полимер и на короткое время погружается в него, формируя углубление. При чтении нагрев производится до меньшей температуры – 300°С, которая недостаточна для размягчения используемого полимерного материала. Благодаря высокой теплопроводности полимера игла при погружении в имеющееся углубление остывает, в результате чего изменяется сопротивление резистора, которое также отслеживается управляющей схемой. При перезаписи данных игла совершает несколько движений с небольшим смещением относительно центра ранее сделанного углубления, как бы разравнивая поверхность полимерного материала.

Удельная плотность записи экспериментальной установки, оснащенной массивом из 1 024 игл, составляет 200 Гбит/кв. дюйм, что позволяет сохранить до 0,5 Гбайт на носителе размером 3 на 3 мм. Один из руководителей проекта Millipede заявил, что в будущем возможно тысячекратное увеличение плотности записи по сравнению с достигнутыми на экспериментальной установке результатами.

Что касается еще одной важной характеристики накопителя – скорости чтения/записи, то у Millipede она ограничена быстродействием игл. «Производительность» одной иглы составляет несколько килобит в секунду, а предельная скорость работы продемонстрированной экспериментальной установки составляет несколько мегабит в секунду. Значительно повысить быстродействие позволит использование более совершенных электронных схем: в ходе экспериментов были достигнуты значительно более высокие показатели – свыше 1 Мбит/с для одной иглы.

При работе со скоростью порядка нескольких мегабит в секунду экспериментальная установка Millipede потребляет около 100 мВт, что сопоставимо с энергозатратами современных модулей флэш-памяти и значительно меньше аналогичного параметра устройств, использующих магнитную запись.

Еще более привлекательными характеристиками обладает носитель NanoMem, о создании которого официально объявила «Rolltronics Corporation». NanoMem – это энергонезависимая молекулярная память, изготавливаемая в виде очень тонкой пленки.

Предваряя описание нового носителя, следует сказать несколько слов о самой корпорации «Rolltronics». Так, одним из основных ее достижений является разработка «рулонного» технологического

процесса для производства различных электронных компонентов, позволившего существенно снизить затраты на их производство, а сами изделия сделать более тонкими, легкими и гибкими. В настоящее время «Rolltronics» и ее партнеры производят тонкопленочные элементы питания, транзисторы, сенсоры, рентгеновские пластины, компоненты OLED – дисплеев и т. п.

Доступная в настоящий момент информация о «начинке» NanoMem весьма скупа: по-видимому, разработчики опасаются за сохранность своего ноу-хау. Известно лишь, что для хранения информации в носителе NanoMem используется слой полимерного вещества и что процедуры записи и чтения осуществляются низковольтными оптоэлектронными сенсорами (помимо электродов и тонкопленочных транзисторов, в структуре носителя NanoMem присутствует тонкий слой светоизлучающего вещества). При записи под действием передаваемого заряда меняется только ориентация молекул – «цилиндров» в пространстве; химический состав полимера при этом не изменяется.

В процессе производства слои носителя NanoMem наносятся на гибкую пластиковую подложку или на металлическую фольгу по фирменной технологии «Rolltronics». Использование технологических достижений «Rolltronics» позволило сократить затраты на производство как минимум в пять раз по сравнению с традиционным процессом.

Если проводить сравнение параметров NanoMem с современными носителями на базе флэш-памяти, то новый молекулярный носитель как минимум на порядок превосходит флэш-память по удельной емкости и при этом обладает значительно меньшей себестоимостью.

«Rolltronics» уже представила первые прототопипы устройств хранения данных, базирующиеся на молекулярной памяти, которые обладают весьма впечатляющими характеристиками. Это модуль PC Card емкостью 64 Гбайт и внешний USB – модуль емкостью 5 Тбайт, имеющий размеры стандартного 3,5-дюймового жесткого диска.

«Вообразите, сколько информации можно уместить в одном носителе формата PC Card стоимостью всего несколько сот долларов. Это и есть наша цель – носители высокой емкости по доступной цене. Мы затратили на исследования несколько лет, но разработанная нашими специалистами молекулярная технология сделала это возможным», – так прокомментировал демонстрацию прототипов председатель Совета директоров компании «Rolltronics». В связи с этим будет уместно привести современные цены на миниатюрные цифровые носители: например, гигабайтная карта CompactFlash Type сейчас стоит около 450 долл., микровинчестер IBM Microdrive такой же емкости – около 250 долл., а недавно анонсированная «Sony» гигабайтная карта Memory Stick – почти 900 долл.

Если говорить о надежности NanoMem, то в ходе тестирования, проведенного доктором Аленом Бардом (Allen Bard) из Техасского университета, были подтверждены следующие данные: абсолютная сохранность данных после отсутствия питания в течение 7 тыс. ч (почти 10 месяцев), а также полное отсутствие ошибок после 1,5 млрд циклов чтения/записи.

Ожидается, что первые серийные изделия на базе NanoMem появятся в продаже уже в 2004 г.

# СОДЕРЖАНИЕ

## Раздел I
## ЗАЩИТА ИНФОРМАЦИИ







## Раздел II
## ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

*НАУЧНОЕ ИЗДАНИЕ*

**ЭКОНОМИКО-ОРГАНИЗАЦИОННЫЕ И ПРОГРАММНО-ТЕХНИЧЕСКИЕ ВОПРОСЫ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ**

**Сборник научных трудов**

Редактор *П. А. Тимачева*
Корректор *Т. О. Гольмдорф*
Компьютерная верстка *О. Д. Мамоновой*

ИД № 00918 от 02.02.2000 г.
Подписано в печать 22.12.03. Формат 60×84 1/16. Бумага типогр. № 1.
Печать цифровая. Усл.-печ. л. 7,25. Уч.-изд. л. 7,0. Изд. № 84. Тираж 300 экз. Заказ 528.

СПбГИЭУ. 191002, Санкт-Петербург, ул. Марата, 27.
ИзПК СПбГИЭУ. 191002, Санкт-Петербург, ул. Марата, 31.