Предложенная методика проведения внутреннего аудита производственных затрат позволяет контролировать своевременность и качество выполнения всех технологических процессов, полноту оприходования продукции молочного скотоводства, калькулирования себестоимости как основных факторов ее снижения.

Б.Я. ТАТАРСКИХ, С.И. АШМАРИНА

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКИХ СИСТЕМ

Проблема информационной безопасности в условиях возрастающего влияния на все сферы человеческой деятельности становится одной из наиболее значимых. Ее необеспеченность способна оказать негативное влияние, сводя на нет усилия по достижению безопасности в широком ее понимании. Появление новых и резкое обострение традиционных проблем информационной безопасности связано также с возрастающими масштабами информатизации как в стране в целом, так и на уровне отдельных регионов. Основными факторами, обусловившими сложившуюся ситуацию, на взгляд авторов, являются следующие:

информационная безопасность в процессе информатизации стала ведущей составляющей в обеспечении национальной безопасности; как показывает опыт последних лет, без информационной безопасности невозможно обеспечить необходимый уровень всех видов национальной безопасности (военной, политической, экономической и т. д.) и надежной безопасности в целом;

информатизация привела к снижению уровня информационной безопасности личности, общества и государства; резко расширился спектр информационных угроз, значительно возросла возможность негативных информационных воздействий.

Ведущая роль информационной компоненты в обеспечении национальной безопасности обусловлена целым рядом объективных обстоятельств, среди которых можно выделить следующие:

разрушение и дезорганизация информационной инфраструктуры страны по силе воздействия на ее органы управления и экономический потенциал соизмеримы с последствиями применения оружия массового поражения;

в условиях прекращения холодной войны и нормализации отношений в традиционной военной области центр тяжести противоборства развитых государств перемещается в информационную сферу;

средства, применяемые для негативных воздействий на информационные и телекоммуникационные системы, стали доступны не только государственным спецслужбам, но и отдельным криминальным и террористическим группировкам, в результате чего проблема информационной безопасности стала международной и по значимости соизмеримой с глобальной экономической и экологической безопасностью.

Однако наибольшую актуальность эта проблема приобретает в связи с обеспечением безопасности информации в вычислительных системах в смысле ее защищенности от воздействий, внешних и внутренних, намеренных или стихийных.

Массовое применение персональных компьютеров и компьютерных сетей в ряде областей человеческой деятельности, среди которых следует выделить такие, как производственная, административная, технологическая, финансовая, патентная и другие (чье информационное наполнение в большей степени не должно быть общедоступным), усиливает значимость проблемы защиты информации и определяет ее возросшую социально-экономическую актуальность.

Борис Яковлевич ТАТАРСКИХ, доктор экономических наук, профессор Самарской экономической академии;

Светлана Игоревна АШМАРИНА, кандидат экономических наук, доцент Самарской экономической академии.

Необходимо особо подчеркнуть значение фактора прогресса. Появление новых технических средств и информационных технологий всегда будет порождать новые аспекты в проблеме защиты информации. Например, слабым местом современных средств обработки данных, способствующим расширению поля угроз, стали сетевые структуры. Здесь уже следует проектировать и применять специальные приемы и средства: разделение ресурсов, скрытые траектории, множественность точек доступа, т.е. использовать принципиально другие подходы, чем в изолированных системах.

Кроме широкого распространения сетевых структур, к революционизирующим факторам современного развития следует также отнести массовое применение вычислительной техники с ограниченным использованием ее ресурсов и индустриализации процесса создания программных средств. Эти факторы также порождают свои аспекты в проблеме защиты.

Таким образом, проблема защиты информации не имеет окончательного решения и речь должна идти о создании условий для постоянного и своевременного отслеживания тенденций и реагирования на них с точки зрения возникновения новых угроз и, возможно, снятия старых.

С учетом существующих тенденций имеются основания говорить о необходимости изменения подхода к проблеме защиты и, прежде всего, оценки защищенности вычислительных систем, в том числе и с позиции оптимизации вложения средств.

Для создания надежных систем обеспечения информационной безопасности необходимы значительные капитальные вложения, которые предназначены для создания материально-технологических средств.

В условиях отсутствия инвестиций в достаточных размерах особо актуальной является проблема оценки эффективности затрат для обеспечения информационной безопасности. В первом приближении это можно сделать, используя формулу,

$$Э_{и.б} = \Delta Р_{и.б} \ / \ \Delta З_{и.б},$$

где $\Delta Р_{и.б}$ — результаты (эффект) от повышения качества обеспечения информационной безопасности (млн р.); $\Delta З_{и.б}$ — совокупные затраты, связанные с обеспечением информационной безопасности (млн р.).

При этом следует учитывать, что в реальных условиях рынка и повышения фактора “коммерческая тайна” темп роста затрат на обеспечение информационной безопасности не может быть меньше темпа затрат на обеспечение требуемой информационной вооруженности управленцев.

Темп вооруженности труда хозяйственных руководителей средствами обеспечения информационной безопасности должен быть несколько выше темпа общей технологической вооруженности.

В целях минимизации затрат на обеспечение информационной безопасности следует учитывать долю “полезной” (защищаемой) информации в общем объеме информационных потоков в производственно-хозяйственных системах.

Обобщенно уровень эффективности использования информационных ресурсов можно представить в виде коэффициента полезного использования информации ($К_{исп.инф}$), определяемого как отношение объема информационного ресурса, использованного при принятии решений, к общему объему информационного ресурса:

$$К_{исп.инф} = И_{р.п.р} \ / \ И_{р},$$

где $И_{р.п.р}$ — объем информационного ресурса, использованного при принятии решений; $И_{р}$ — общий объем информационного ресурса.

Для управления эффективностью информационных ресурсов и, как следствие, эффективностью процедур обеспечения информационной безопасности, на уровне предприятия (объединения) можно принять следующее неравенство (экономическую нормаль):

$$J_{п(g)} > J_{и.в} > J_{о.т.в} > J_{р},$$

где $J_{п(g)}$ — индекс роста прибыли; $J_{и.в}$ — индекс роста информационной вооруженности; $J_{о.т.в}$ — индекс роста общей технической вооруженности; $J_{р}$ — индекс численности рабочих в системе управления предприятием.

В связи с оценкой затрат на обеспечение информационной безопасности целесообразно определить резервы повышения эффективности информатизации ($Р_{эф.инф}$) в общем виде по формуле

$$Р_{эф.инф} = Э_{и.р} / Э_{и.т},$$

где $Э_{и.р}$ — эффект информатизации реализованный (фактически достигнутый); $Э_{и.т}$ — эффект информатизации максимально возможный (теоретический).

Коэффициент развития информатизации может быть определен по формуле

$$К_{инф} = У_{инф.ф} / У_{инф.б},$$

где $У_{инф.ф}$ — уровень развития информатизации достигнутый (фактический); $У_{инф.б}$ — уровень развития информатизации базовый (максимально возможный).

В целом обеспечение защиты информации в процессе информатизации должно, на взгляд авторов, включать следующие аспекты:

- формирование организационной структуры системы защиты информации и проведение организационных мероприятий;
- сертификацию аппаратных средств защиты информации систем связи и вычислительной техники;
- защиту баз данных от несанкционированного доступа с использованием идентификационных (магнитных, голографических и др.) карточек и высоконадежной системы паролей;
- разработку и создание интегрированной информационно-вычислительной сети с многоуровневой организацией защиты информации;
- разработку и внедрение высокозащищенных информационных технологий с малым числом уровней защиты, например волоконно-оптических линий и т.п.;
- принятие нормативных актов о стандартизации программных средств защиты, использование лицензионного программного обеспечения;
- проведение научных исследований для создания высокоэффективных аппаратно-программных средств защиты информации;
- стандартизацию и сертификацию программных средств защиты (антивирусных, криптографических, паролей) систем связи и вычислительной техники;
- разработку систем контроля и управления доступом интегрированных баз данных;
- разработку и внедрение многоуровневой системы защиты интегрированной информационно-вычислительной сети.

С учетом вышеперечисленных критериев обоснования оптимизации затрат построение технологий информационной безопасности требует разработки специальной методологии, позволяющей не ограничиваться простым выбором технических и организационных решений, а концентрировать внимание разработчиков и пользователей на таких составляющих, как кадровое, организационно-техническое и технологическое обеспечение.

Общая схема построения системы информационной безопасности должна включать 5 последовательных этапов: подготовительный, аналитический, исследовательский, рекомендательный и этап внедрения.

На подготовительном этапе выбираются и обосновываются объект (автоматизированные информационные системы (АИС) в целом, отдельные компоненты), цели и задачи, общая концепция системы безопасности.

Основной задачей аналитического этапа является сбор, систематизация и обработка информации о потенциальных угрозах, каналах утечки информации, а также разработка эталонов и критериев эффективности защиты информации, рассмотрение характеристик существующих аппаратно-программных средств защиты.

На исследовательском этапе определяется политика безопасности, допустимая степень риска, набор процедур и методов несанкционированного доступа к ресурсам АИС.

Содержание рекомендательного этапа заключается в дальнейшей проработке вариантов размещения элементов системы информационной безопасности АИС, выборе оптимального варианта по критерию “эффективность — стоимость”, документировании, оформлении окончательных рекомендаций к внедрению.

Этап внедрения включает в себя работы по обучению персонала, дальнейшее развитие и поддержку составных частей системы информационной безопасности, а также регулярное тестирование.

Эффективность построенных таким образом систем информационной безопасности достигается за счет тесного взаимодействия с существующими автоматизированными информационными системами, а также благодаря глубокому мониторингу внешних и внутренних информационных источников по проблемам информационной безопасности.

Построенная по предложенной схеме система информационной безопасности позволяет прежде всего предотвращать программные злоупотребления, а также уменьшает потенциальную опасность потери любого вида ресурсов.

В целом система информационной безопасности любых экономических структур должна учитывать следующие требования:

1. Структура построения систем защиты производств информации должна разрабатываться синхронно с созданием самих производственных информационных систем (ИС), с учетом разграничения специфики информации по степени важности и полноты доступности. В особых случаях системе защиты информации должна быть отведена ведущая роль по отношению к информационным системам. При этом предварительно и однозначно должны определяться цель и критерии защиты, а модель защиты следует сделать по возможности полной и связной. Решение задачи по защите информации должно быть в некотором смысле оптимизировано (учтена специфика построения не только ИС, но и информационных управленческих структур), а следовательно, целенаправленно и целесообразно, и лишь тогда оценка относительной защищенности информации объекта станет объективно-содержательной;

2. Современные условия требуют изменение подхода и решению вопросов обеспечения информационной безопасности, разработки систем информационной безопасности, адекватно реагирующих на изменяющиеся требования и качеству, и структуре процедур, обеспечивающих информационную безопасность. Необходимы широкие функциональные исследования безопасности открытых ИС, а также мониторинг достижений в области обеспечения информационной безопасности;

3. Без развития региональных баз данных, в состав которых должны входить центры переработки информации (при включении в мировое информационное пространство), достижение достаточного уровня информационной безопасности как на национальном, так и на корпоративном уровнях, невозможно;

Кроме того, решение поставленной проблемы должно предусматривать процедуры обеспечения информационной безопасности соотносительно с требованиями мирового стандарта по защите определенных категорий информационной продукции. Применительно к нашим рыночным условиям хозяйствования значительная часть информации как внутри производственного, так и внешнего назначения является закрытой для потенциальных инвесторов и для участников рынка;

4. Необходима разработка мероприятий по достижению минимизации затрат на системы информационной безопасности путем более детальной градации информации по шкале ценностей, использования процедур прогнозирования долгосрочности и важности информационной продукции (на основе изучения жизненного цикла информации);

5. В целом проектирование защиты информационных объектов открытых систем должно исходить из фундаментальных свойств самого исследуемого объекта. Стремление обеспечить защищенность путем ужесточения изоляции ЛВС чревато возникновением плохо предсказуемой опасности.

Предложенные меры позволят значительно повысить не только информационный, но и экономический эффект любой предпринимательской деятельности.