

И.Е. Илякова, И.А. Григорьянц
I.E. Ilyakova, I.A. Grigoriyants

**РОЛЬ ЭФФЕКТИВНОЙ СИСТЕМЫ ИНФОРМАЦИОННОГО
ОБЕСПЕЧЕНИЯ В СИСТЕМЕ ИНДИКАТИВНОГО ПЛАНИРОВАНИЯ
ЭКОНОМИЧЕСКОГО РАЗВИТИЯ ОРГАНИЗАЦИИ**
**THE ROLE OF AN EFFECTIVE INFORMATION SUPPORT
SYSTEM IN THE SYSTEM OF INDICATIVE PLANNING OF
AN ORGANIZATION'S ECONOMIC DEVELOPMENT**

Аннотация:

В условиях развития информационных технологий, в эпоху цифровой экономики облегчается доступ внутри организации ко всей информации, которая необходима для принятия эффективного, своевременного управленческого решения. Информационные потоки внутри организации можно перенаправить исходя из сиюминутной необходимости организации, а также, конечно, из требований ситуационного и стратегического планирования. Возможным это становится за счет создания информационной системы работы предприятия, в которой и аккумулируется информация, необходимая для эффективной, слаженной работы и четкого взаимодействия всех подразделений предприятия. Таковых информационных систем на сегодняшний день разработано достаточно много, и каждая организация может в соответствии со своими потребностями и спецификой деятельности подобрать информационную систему согласно обозначенным нуждам. Более того, все информационные системы имеют возможность трансформироваться, дополняться согласно возникающим потребностям в каждый конкретный момент работы организации. Важные для деятельности организации характеристики информационных систем, обеспечивающих в итоге высокую конкурентоспособность предприятия — это быстрота сбора и обработки информации, ее доступность всем необходимым подразделениям для принятия управленческих решений.

Для эффективности работы информационной системы важно пройти несколько этапов при ее выстраивании, чтобы максимально адаптировать под специфичность деятельности организации. В этом случае можно говорить об эффективности системы, ее структуры уже на этапе построения.

Однако любая информационная система уязвима и требует обеспечения собственной безопасности. В связи с этим следует предпринять ряд мер для устранения возможной уязвимости информационной системы предприятия с целью предотвращения, в частности, утечки информации, составляющей коммерческую тайну, и утраты в результате этого достигнутых позиций на рынке.

Ключевые слова: информация, безопасность, система, управление, ресурсы, риск, индикативное планирование.

Abstract:

In the context of the development of information technologies, in the era of the digital economy, access within the organization to all the information that is necessary for making an effective, timely management decision is facilitated. Information flows within an organization can be redirected based on the immediate need of the organization, as well as, of course, based on situational and strategic planning. This becomes possible due to the creation of an information system for the work of the enterprise, in which the necessary information is accumulated for effective, well-coordinated work and clear interaction of all departments of the enterprise. There are quite a lot of such information systems developed today and each organization is able to choose an information system according to its needs and the specifics of its activities according to the designated needs. Moreover, all information systems have the opportunity to be transformed, supplemented according to the emerging needs at each individual moment of the organization's activity. Important characteristics of the information systems of the organization's activities are the speed of collecting, processing information, its availability to all necessary departments for making managerial decisions, which ultimately ensure the high competitiveness of the organization.

For the effectiveness of the information system, it is important to go through several stages when building it in order to adapt it as much as possible to the specifics of the organization's activities. In this case, we can talk about the effectiveness of the system, its structure is already at the stage of construction.

However, any information system is vulnerable and requires its own security. In this regard, a number of measures should be taken to eliminate the possible vulnerability of the enterprise's information system in order to prevent, in particular, the leakage of information constituting a trade secret and the loss of market positions achieved as a result.

Keywords: information, security, system, management, resources, risk, indicative planning.

Управление современным предприятием предполагает использование автоматизированных систем комплексного учета.

Менеджеры предприятий принимают множество управленческих решений на основе той информации, которую они черпают из информационных систем. Сегодня для предприятия важно единое информационное пространство, поскольку оно объединяет все сферы

деятельности организации — бухгалтерский учет, учет всех договоров предприятия, учет движения материальных ценностей и т. д.⁵⁰

Для создания более эффективной системы принятия управленческих решений и создается информационная система, которая должна включать в себя:

— систему внутреннего учета, в которой должны быть данные об объеме производства товаров (услуг), об издержках производства, доходах и прочие финансовые показатели;

— информатизацию маркетинговых процессов предприятия — это учет продаж, отслеживание тенденций на рынке, работа с потребительской аудиторией, учет деятельности конкурентов, сбор и обработка данных и многое другое.

Информационная система наполняется посредством внесения соответствующих данных либо автоматически, либо вручную персоналом. На основании этих данных и принимаются тактические и стратегические решения, влияющие как на функционирование, так и на развитие организации⁵¹.

Кроме того, данные, которые накапливаются в информационной системе предприятия, дают полноценную картину его деятельности, что очень важно для менеджмента при принятии правильных управленческих решений⁵².

Различные подразделения предприятия видят лишь часть всей картины деятельности организации, внося свои данные в общую информационную систему. Менеджерам же необходимо видение общей ситуации, так как только с учетом имеющихся в информационной системе индикаторов деятельности организации становится возможным принятие своевременного и выверенного управленческого решения, на основе которого происходит индикативное планирование.

Однако любая информационная система имеет точки уязвимости. От риска не застрахована ни одна информационная система, ни одно предприятие. С точки зрения развития организации, ее рыночных пози-

⁵⁰ Волкова К.С., Мудрова С.В. Стратегическое планирование как основа развития России // Проблемы и перспективы развития промышленности России. Сб. материалов XI Международной научно-практической конференции / Под ред. А.В. Быстрова. М., 2022. С. 98—104.

⁵¹ Минаева В.М. Индикативное планирование экономической безопасности в условиях цифровизации // Студенческая наука — взгляд в будущее. Материалы XVII Всероссийской студенческой научной конференции. Красноярск, 2022. С. 158—161.

⁵² Климова П.А., Афонина Я.В. Особенности стратегического планирования в условиях кризиса // Сборник научных работ серии «Экономика». Донецк, 2022. № 28. С. 140—147.

ций, неправильно реагировать на уже произошедший факт сбоя информационной системы, так как вследствие этого теряется вся первостепенная значимость важной информации, которую получают менеджеры, — главное стратегическое «оружие» организации. Таким образом, в каждой организации необходимо создавать систему информационной безопасности. Это такая же неотъемлемая часть системы управления, как и сама информационная система: нарушение работы или, что еще хуже, полная остановка работы информационной системы могут иметь необратимые последствия для организации — это потеря времени, ресурсов, сбой в работе с целевой аудиторией и в итоге проигранная конкурентная борьба.

Вариант информационной базы (системы) обеспечения управленческого процесса в организации представлен на Рисунке 1.



Рис. 1. Информационная база аппарата управления организацией.

Угрозы развитию организации могут быть как внешние, так и внутренние.

Внешние угрозы чаще всего исходят от конкурентов. Информационная система предприятия может быть поражена вследствие разнообразных хакерских атак, сама информация может быть подвергнута частичной порче либо полному уничтожению⁵³. Крупные компании могут

⁵³ Брче М.А., Шааб А., Шааб А. Цифровизация в практической реализации концепции устойчивого развития // Век XXI. Цифровизация: вызовы, риски, перспективы. Материалы международной научно-практической конференции. Сер.

также столкнуться с действиями в отношении персонала организации, а именно подкупом, шантажом и пр., имеющими целью получение информации, которая составляет коммерческую тайну и имеет первостепенную важность для предприятия. Существует и более легальный способ получения информации конкурента — перемаивание хорошего специалиста в другую компанию. Таким образом организация получает и ценного сотрудника, и важную информацию о конкуренте, которой этот сотрудник обладает. Это явление уже из области хедхантерства⁵⁴.

Не менее опасны и внутренние угрозы. Они могут являться следствием некомпетентности руководства, недостаточной квалификации персонала либо устаревания средств информационных технологий, которые составляют основу информационной системы организации, компьютерные вирусы, в том числе умышленно занесенные. Менеджмент организации порой упускает из виду часть сотрудников, которые могут быть чем-то не удовлетворены, например, уровнем заработной платы, условиями труда, вследствие чего они могут разгласить коммерческую тайну организации.

Таким образом, ущерб информационным ресурсам предприятия может быть нанесен вследствие:

- несанкционированного доступа и хищения конфиденциальной информации;
- перехвата информации из систем связи организации;
- незаконного прослушивания конфиденциальных переговоров;
- неосторожного обращения сотрудников с конфиденциальной информацией;
- подкупа сотрудников организации.

Основные источники информации — это персонал организации, ее документы, продукция, технические средства информации⁵⁵.

Среди главных направлений защиты информации можно выделить:

«VIII Декартовские чтения». М.; Зеленоград, 2022. С. 45—51.

⁵⁴ Михайлова Л.В., Авхадиев Ф.Н., Неверова П.В. Индикативное планирование в российской экономике // Актуальные проблемы бухгалтерского учета и аудита в условиях стратегического развития экономики. Сб. научных трудов по материалам Всероссийской (национальной) научно-практической конференции молодых ученых. Казань, 2022. С. 733—739.

⁵⁵ Борисов А.Ю. Перспективы использования индикативного планирования в современной России // Актуальные аспекты развития науки и общества в эпоху цифровой трансформации. Сб. материалов III Международной научно-практической конференции. М., 2022. С. 247—251.

- защита информации юридическими средствами (государственное законодательство, внутренние локально-нормативные акты организации, документированный перечень сведений, составляющих коммерческую тайну организации и не подлежащих разглашению);
- обязательства сотрудников организации по неразглашению информации, составляющей коммерческую тайну (внутренние распоряжения, памятка сотрудникам);
- организационные мероприятия, позволяющие защитить значимую для предприятия информацию (создание службы информационной безопасности, режимность и пропускная система на предприятии, закрепленная внутренними локально-нормативными актами, должная организация работы с документами);
- техническая защита информации (различные технические и программно-аппаратные средства защиты).

Структура информационного обеспечения организации представлена на Рисунке 2.



Рис. 2. Структура системы информационного обеспечения организации.

При защите информации необходимо исходить из того, что сама организация такой работы должна строиться на принципах комплексности использования средств и методов защиты. Невозможно и нецелесообразно использование только одного какого-либо средства, даже

с высокой степенью надежности. Необходимо системное согласование нескольких средств защиты информации^{56,57}.

Менеджмент организации должен осознавать всю важность информационной безопасности, прогнозировать будущее развитие событий, предвидеть тенденции в области защиты информации и отслеживать новые способы хищения конфиденциальной информации. Эффективная работа системы информационной безопасности должна стать важнейшей, одной из первоочередных задач всего предприятия.

Обеспечение информационной безопасности предприятия следует организовывать, последовательно реализуя следующие этапы:

Определение основ формирования информационной безопасности. На данном этапе необходимо сформулировать цель, стратегию информационной безопасности организации, определить принципы и методы управления информационной безопасностью. Также данный этап включает в себя определение объекта и субъекта управления информационной безопасностью.

Анализ факторов внешней и внутренней среды на предмет исходящих угроз. Целесообразно максимально точно идентифицировать все риски и угрозы для информационной безопасности предприятия, влияющие или могущие повлиять на его устойчивое развитие.

Исходя из проделанной на предыдущем этапе работы, необходимо оценить и выявить основные наиболее важные угрозы для информационной системы предприятия и сопоставить их с потенциалом безопасности создаваемой информационной системы.

Определить основные показатели, характеризующие систему информационной безопасности, главные индикаторы, на основе которых можно делать вывод о надежности создаваемой системы.

Выработка управленческого решения о создании и начале функционирования информационной системы безопасности организации, с перечислением основных рисков, целей и функций созданной системы, т. е. с полноценным описанием процесса обеспечения стабильной работы системы информационной безопасности.

⁵⁶ Колесников В.В., Макаров И.Н., Цоголакян Л.Д. Индикативное планирование в европейских экономиках // Саяпинские чтения. Материалы VI Всероссийской (национальной) научно-практической конференции / Отв. ред. А.А. Бурмистрова, А.В. Саяпин, Н.К. Родионова. Тамбов, 2023. С. 48—53.

⁵⁷ Никитина Л.Н., Осипова Э.Н., Флягина Т.А. Экономико-математическое моделирование в принятии оптимальных управленческих решений. Показатель индикативности // Известия высших учебных заведений. Технология текстильной промышленности. 2022. № 1 (397). С. 5—11.

Приведенная выше последовательность представляет собой общую поэтапную схему механизма создания и обеспечения информационной системы безопасности предприятия. Детализация данного механизма зависит уже от специфики организации. В каждом конкретном случае он может быть адаптирован под условия любой организации.

Определим основные характерные черты данного механизма обеспечения информационной безопасности:

- гибкость и постоянное совершенствование всех его составляющих, адаптация под сложившиеся условия в каждый конкретный момент времени на основе анализа их эффективности;
- адаптивность по отношению к условиям внешней и внутренней среды организации.

В данном механизме важно четко определить все составляющие его элементы и проанализировать их взаимодействие между собой. Механизм обеспечения информационной безопасности станет эффективным лишь в том случае, если его структура будет включать в себя ряд блоков, состоящих из следующих элементов:

- постоянный мониторинг состояния организации с целью своевременного предотвращения возникающих угроз;
- определение регламента работы службы безопасности предприятия по выявлению возникающих угроз;
- определение значений показателей, при которых явно возникает угроза деятельности предприятия.

Механизм обеспечения информационной безопасности, помимо защиты, должен также выполнять еще несколько важных функций — регулятивную, предупредительную, инновационную и др.

Безусловно, выполнение защитной функции является важнейшей и основной задачей системы обеспечения информационной безопасности. Для ее реализации необходимы следующие условия:

- наличие соответствующего кадрового потенциала организации;
- наличие соответствующего экономического потенциала организации;
- развитие человеческого капитала организации;
- защита самой организации от внешних угроз.

Регулятивная функция призвана вносить последовательность и порядок в функционирование организации при ее взаимодействии с внешней средой. Здесь должны учитываться в первую очередь такие условия внешней среды, как уровень конкуренции и ценовая ситуация на рынке.

Предупредительная функция призвана обеспечить прогнозирование ситуации на рынке и вероятное влияние на нее предприятия,

а также обеспечить превентивные действия в случае возникновения внешних и внутренних угроз. В связи с возможным возникновением таких угроз после предупредительных мероприятий необходима выработка мер противодействия экономического, технологического, организационного характера. Разработка прогнозов и предупредительных мероприятий основывается на информационной составляющей данного механизма безопасности, обеспечивающего менеджмент предприятия достоверной и своевременной информацией.

Инновационная функция призвана обеспечить разрешение назревающих неблагоприятных ситуаций инновационными методами.

Индикаторы информационной безопасности предприятия — это нормативные показатели его деятельности, которые сообщают об угрозах и настолько чувствительны, что заблаговременно предупреждают о возникающей опасности. Количественные показатели имеют здесь первостепенное значение, поскольку именно они определяют наиболее уязвимые точки в работе организации. На основании количественных данных можно определить и потенциальные последствия возникающих угроз.

С точки зрения целостной, системной картины управления организацией, результаты анализа угроз предприятию также могут послужить основой для решения ряда назревающих внутренних проблем в таких областях деятельности менеджмента, как планирование, организация, мотивация.

Таким образом, важнейшим этапом деятельности информационной системы любой организации должно быть выявление первых признаков кризисной ситуации — с тем чтобы можно было вовремя реализовать предупредительные меры, направленные на нейтрализацию и предотвращение развития кризисной ситуации, и чтобы затрата ресурсов на восстановление стабильной работы оказалась минимальна.

Список литературы

1. *Борисов А.Ю.* Перспективы использования индикативного планирования в современной России // Актуальные аспекты развития науки и общества в эпоху цифровой трансформации. Сб. материалов III Международной научно-практической конференции. М., 2022. С. 247—251.

2. *Брче М.А., Шааб А., Шааб А.* Цифровизация в практической реализации концепции устойчивого развития // Век XXI. Цифровизация: вызовы, риски, перспективы. Материалы международной научно-практической конференции. Серия «VIII Декартовские чтения». М.; Зеленоград, 2022. С. 45—51.

3. Волкова К.С., Комолов О.О., Мудрова С.В. Международный опыт применения индикативного планирования в посткризисный период // Экономика: вчера, сегодня, завтра. 2022. Т. 12. № 10-1. С. 457—467.

4. Волкова К.С., Мудрова С.В. Стратегическое планирование как основа развития России // Проблемы и перспективы развития промышленности России. Сб. материалов XI Международной научно-практической конференции / Под ред. А.В. Быстрова. М., 2022. С. 98—104.

5. Климова П.А., Афонина Я.В. Особенности стратегического планирования в условиях кризиса // Сборник научных работ серии «Экономика». Донецк, 2022. № 28. С. 140—147.

6. Колесников В.В., Макаров И.Н., Цоголакян Л.Д. Индикативное планирование в европейских экономиках // Саяпинские чтения. Материалы VI Всероссийской (национальной) научно-практической конференции / Отв. ред. А.А. Бурмистрова, А.В. Саяпин, Н.К. Родионова. Тамбов, 2023. С. 48—53.

7. Минаева В.М. Индикативное планирование экономической безопасности в условиях цифровизации // Студенческая наука — взгляд в будущее. Материалы XVII Всероссийской студенческой научной конференции. Красноярск, 2022. С. 158—161.

8. Михайлова Л.В., Авхадиев Ф.Н., Неверова П.В. Индикативное планирование в российской экономике // Актуальные проблемы бухгалтерского учета и аудита в условиях стратегического развития экономики. Сб. научных трудов по материалам Всероссийской (национальной) научно-практической конференции молодых ученых. Казань, 2022. С. 733—739.

9. Никитина Л.Н., Осипова Э.Н., Флягина Т.А. Экономико-математическое моделирование в принятии оптимальных управленческих решений. Показатель индикативности // Известия высших учебных заведений. Технология текстильной промышленности. 2022. № 1 (397). С. 5—11.

Сведения об авторах

Илякова Ирина Евгеньевна, кандидат экономических наук, доцент, Московский государственный университет технологий и управления им. К.Г. Разумовского. E-mail: ir.ilyakova@mgutm.ru

Григорьянц Игорь Александрович, кандидат экономических наук, Самарский национальный исследовательский университет им. С.П. Королева.