ляється коригування плану. При цьому аналіз результатів повинен включати оцінку слабких і сильних місць рішення і планів його реалізації, додаткових ризиків. Результати проведеного аналізу можуть вплинути на переоцінку можливостей підприємства і привести до зміни його стратегії і місії.

## ВИСНОВКИ

Оскільки безпека, як ресурс підприємства, в більшості випадків є платною, то при виникненні загроз і ризиків підприємство вимушене використовувати частину своїх активів, що забезпечують певну прибутковість, не у виробничій діяльності, а в цілях забезпечення безпеки. При ухваленні рішень, з урахуванням безпеки, керівництво підприємства вимушене оцінювати також альтернативні витрати після різних засобів забезпечення безпеки. Придбання ресурсу безпеки фінансово - господарської діяльності може вимагати значних фінансових коштів. У той же час, існує можливість вибору, наприклад, між використанням факторингу, страхуванням кредитних ризиків і змістом власної служби безпеки, з метою погашення дебіторської заборгованості; не менш ефективним, але економнішим засобом забезпечення збереження майна підприємства, чим використання послуг.

Отже, джерело більшості загроз економічної безпеки підприємств слід шукати в ухваленні помилкових управлінських рішень, а рішення проблеми забезпечення безпеки господарюючого суб'єкту є в адекватному застосуванні існуючих методів антикризового і антиризикового управління. Розвиток засобів забезпечення безпеки відбувається з орієнтацією як на запобігання втратам ресурсів підприємства шляхом введення нових засобів захисту і контролю, так і на підвищення продуктивності праці і ефективності бізнес-процесів, на розширення асортименту продукції через диверсифікацію виробництва і випуск нових (інноваційних) продуктів.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Асаул А. Н. Организация предпринимательской деятельности / А. Н. Асаул. — СПб.: Питер, 2005. —368 с.

2. Гапоненко В.Ф. Экономическая безопасность предприятия / В.Ф. Гапоненко, А.Л. Беспалько, А.С. Власков. — М.: Издательство «Ось-89», 2007. — 208 с.

3. Матвійчук А.В. Аналіз і управління економічним ризиком / А.В. Матвійчук. — К.: Центр навчальної літератури, 2005. — 347 с.

4. Литвак Б.Г. Наука управления. Теория и практика. / Б.Г. Литвак. — М.: Дело, 2011. — 423 с.

5. Соснин А.С. Менеджмент безопасности предпринимательства: учеб. пособие. / А.С. Соснин, П.Я. Прыгунов. — К.: Изд-во Европ. Ун-та, 2002. — 125 с.

УДК 658(005.934)

## СТРУКТУРА КОНТУРА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

*Гончаренко Ю.Ю.*

*Рассматривается понятие информационной безопасности в рамках управления предприятием и оценивается структура контура управления как совокупность формальных управленческих процедур.*

***Ключевые слова:*** *предприятие, управление, информация, информационная безопасность предприятия.*

Руководителю любого предприятия нужна полная картина, отражающая состояние его предприятия, высокий уровень управляемости и осознание перспектив развития рынка и бизнеса [1].

Система управления предприятием в первом приближении состоит в стратегическом управлении, управлении финансами, управленческом контролинге и управлении персоналом [2]. Управление предприятием – это многофакторный процесс, успешность которого определяется подготовкой персонала, наличием современного оборудования, применением новых технологий, компетентностью руководителя [3]. Развитие современных систем обработки, систематизации и анализа информации, базы персональных электронных вычислительных машин, средств радио и телекоммуникаций, информационных технологий обеспечивают взаимодействие и воздействие на партнеров и конкурентов без вступления с ними в непосредственный контакт [4]. В свою очередь, это обуславливает появление новой научной и организационно-технической проблемы – информационной безопасности предприятия.

Информационная безопасность является одной из составляющих обеспечения безопасности предприятия и его деятельности в целом. В общем случае информационная безопасность включает в себя защиту и сохранение коммерческой тайны предприятия, сведений об особенностях производства и сбыта продукции, обеспечение конфиденциальности документооборота, сохранение конфиденциальности личных данных штатных сотрудников, а также лиц, оказывающих содействие разовыми или регулярными консультациями и информационно-технической поддержкой [5]. Информационная безопасность не является какой-то постоянной субстанцией. Она, обеспечивая решение конкретных задач, находится в динамическом состоянии в зависимости от постоянно меняющихся параметров внешней и внутренней обстановки [6]. Процесс адаптивного изменения в зависимости от внешних и внутренних условий принято называть процессом управления информационной безопасностью [7]. В то же время любой процесс управления предусматривает наличие определенных формальных процедур, объединенных понятием «контур управления» [8].

Целью данной работы является выявление особенностей структуры контура управления информационной безопасностью предприятия. Для достижения поставленной цели необходимо решить следующие задачи: первоначально проанализировать суть и содержание понятия информационной безопасности предприятия как основного объекта управления, затем рассмотреть структуру контура управления информационной безопасностью предприятия в целом.

Управление – это сложная интеллектуальная деятельность человека, требующая специальных знаний и опыта. Качества руководителя предприятия, как управляющего процессом производства, включают ряд аспектов. Это знание теории управления, обладание энергией, здоровой психикой, умением применять знания, желанием эффективно работать. Управление в условиях рыночной экономики означает ориентацию предприятия на спрос и потребности рынка, стремление к повышению эффективности производства, хозяйственная самостоятельность, свобода принятия решений, постоянная корректировка целей и задач в зависимости от состояния рынка. Сущность управления – установление и поддержание согласованности взаимодействия людей, участвующих в едином процессе.

Предприятие как производитель определенной продукции или услуг в общем случае содержит технические средства производства, средства их обеспечения и персонал. К техническим средствам производства относятся земельные участки, здания и сооружения, специальное оборудование, производящее определенную продукцию, транспорт, сырье, вовлеченное в процесс производства, а также часть готовой продукции, складируемой для последующей транспортировки. Средства, обеспечивающие соответствующий процесс производства, можно разделить на два вида: коммунально-бытовые и коммуникационные. К первой группе относится обеспечение предприятия электроэнергией, водой, канализацией, очистными сооружениями, столовыми, бытовыми помещениями и т.д. Ко второй – связь (проводная, радио и радиорелейная) и транспорт (автомобильный, железнодорожный, водный, трубопроводный, авиационный и т.д.) Эксплуатирует все указанные выше средства персонал, действиями которого в конечном итоге и создается готовая продукция предприятия. Условно эта часть его деятельности считается внутренним процессом, происходящим на локальном участке контролируемой территории.

Само по себе, обособленно, предприятие функционировать не может. Для выполнения всех внутренних процессов необходимы еще два элемента. Первый – это поставки или входные про-

цессы, второй – исходящие процессы, то есть реализация основной и второстепенной (побочной) продукции. К поставкам относятся, прежде всего, все виды необходимого сырья, техническое оборудование, технологии, а также прием на работу новых сотрудников. Исходящие процессы включают в себя доставку всех видов продукции потребителям или посредникам, осуществляющим ее сбыт, все виды отходов и антропогенных загрязнений, являющихся последствиями производственной деятельности, а также увольнение сотрудников предприятия.

К особому, финансовому, аспекту входных и выходных процессов относятся платежи, осуществляемые предприятием, и поступление средств на его счета.

Для всех процессов (внутренних, входящих, исходящих), сопровождающих деятельность предприятия, характерно наличие информационной составляющей, которая в той или иной степени с ними соприкасается и является частью коммерческой тайны. Независимо от вида информации, связанной с обеспечением того или иного процесса действующего производства, для нее (информации) характерно наличие трех свойств, а именно: конфиденциальность, целостность и доступность.

Конфиденциальность или закрытость (секретность) объясняется тем, что каждый исполнитель должен знать ровно столько сведений, сколько необходимо для выполнения его функциональных обязанностей.

Целостность – это свойство информации, которое обеспечивает исполнителю понимание его места и роли в процессе производства и позволяет лучше исполнять свои обязанности.

Доступность – это свойство информации, позволяющее исполнителю получать основные и вспомогательные сведения, необходимые в процессе производства.

Обеспечение выполнимости всех трех свойств в отношении информации, сопровождающей весь процесс производства на предприятии, принято определять как информационную безопасность предприятия.

Безусловно, любое предприятие не находится в вакууме. Рынок в общем случае формируется наличием поставщиков и потребителей, партнеров и конкурентов, контролирующих инстанций и общественных организаций, законодательной базой и т.п. В связи с этим оценку текущего состояния информационной безопасности предприятия необходимо осуществлять постоянно путем мониторинга, т.е. сбора, обработки, анализа и систематизации циркулирующей информации, которая условно в общем случае подразделяется на четыре вида. Первые три сопровождают входящие, исходящие и внутренние процессы на предприятии, а четвертый относится к его персоналу.

Систематизация информации позволяет выявить любые отклонения от нормы в происходящих процессах, что, в свою очередь, должно послужить сигналом для начала определенной аналитической работы, состоящей в моделировании всех возможных вариантов развития событий. На основании выполненных прогностических рассуждений, а в ряде случаев и прогностических расчетов, разрабатываются предложения по обеспечению конфиденциальности, целостности и доступности информации. Выработанная стратегия докладывается руководителю предприятия или другому лицу, уполномоченному принимать соответствующее решение. После того, как руководство определится с решением, оно в виде приказов, инструкций, распоряжений или в других формах доводится до исполнителей, обязанных их строго выполнять. Другими словами, происходит воздействие на объект управления – информационную безопасность предприятия.

Последующий мониторинг показывает, насколько эффективно это воздействие: вернулись ли информационные показатели процессов в первоначальное состояние или требуется дополнительная корректировка.

Под организацией понимается структура (состав), в рамках которой проводятся сознательно координируемые мероприятия, направленные на достижение общих целей. Организация – анатомия предприятия. Управление – физиология. Структура организации – это логические взаимоотношения уровней управления и функциональных областей, построенные в такой форме, которая позволяет наиболее эффективно достичь целей предприятия. Организация не может функционировать изолированно. Внутренняя среда – это цели, организационная структура, задачи, технология, люди; внешняя среда – клиенты, конкуренты, банки, поставщики, учреждения и т.д.

Организационные связи – те коммуникации, которые существуют между работниками аппарата управления и не опосредованы устойчивой зависимостью между ними, а в основном только единством реализуемых ими целей. Основу процесса управления составляет взаимодействие между элементами управленческой структуры – подразделениями, должностями, отдельными лицами. По содержанию такое взаимодействие может быть информационным, административным или техническим. В рамках информационного взаимодействия осуществляется обмен сведениями, необходимыми для принятия решений. Административное взаимодействие – это управленческие полномочия и ответственность, распоряжения, приказы, рекомендации, отчеты и процесс контроля. Техническое взаимодействие реализуется через совместное участие в практической деятельности (обмен опытом, проведение совещаний и т.п.). Отношения внутри организации могут быть формальными и неформальными. Первые связывают должности или подразделения, вторые – частных лиц. По формальным каналам осуществляется передача только формальной (служебной) информации. По неформальным – как официальной, так и личной. Если отношения связывают элементы структуры, принадлежащие к ее различным уровням, то они являются вертикальными, а если к одному – горизонтальными. По вертикали сверху вниз передаются команды и инструкции, в обратном – отчеты о проделанной работе, советы или рекомендации. Горизонтальные каналы непосредственно связывают равные по положению или статусу элементы организации, обеспечивают наиболее эффективное решение общих проблем за счет оперативности, возможности действовать инициативно и самостоятельно.

Линейная структура одна из простейших организационных структур управления, она образуется в результате построения системы управления на основе только вертикальных связей между звеньями системы управления в виде иерархической лестницы. Она характеризуется тем, что во главе каждого структурного подразделения находится руководитель единоначальник, наделенный всеми полномочиями, осуществляющий единоличное руководство подчиненными ему работниками и сосредотачивающий в своих руках все функции управления. При этом каждый работник подчиняется только одному руководителю и, следовательно, связан с более высокими уровнями управления только через своего непосредственного начальника.

С развитием производства и возрастанием его требований к качеству решаемых самых различных задач управления возникла необходимость в выделении органов управления, специализирующихся на выполнении отдельных функций управления. Происшедшая вследствие этого специализация и кооперация труда в аппарате управления привела к созданию функциональной организационной структуры. В такой организационной структуре функциональному руководителю делегируется линейная власть в масштабе выполняемой функции управления. Разновидностью функциональной структуры, является линейно-функциональная структура управления. В этой структуре сочетаются преимущества линейной и функциональной структур, но доминирующими остаются вертикальные (командные) связи типа «руководитель-подчиненный». Функциональные звенья управления лишены административной власти в отношении нижестоящих исполнителей и руководителей, функциональные руководители вышестоящих уровней осуществляют лишь функциональное руководство нижестоящими функциональными службами.

Контур управления информационной безопасностью соответствует всей системе управления предприятием и реализует три вида целей: стратегические (долговременные), текущие (как правило, до года) и оперативные (до месяца). Он обеспечивает выполнение функций планирования, организации и координирования (регулирования) информационной безопасностью, стимулирование (мотивация) персонала на соблюдение необходимых организационных и технических мер, учет (фиксация состояния управляемого объекта) всех носителей информации, анализ состояния информационной безопасности (выявление причин и предпосылок утечки информации или ее повреждения), а также контроль (выработка мер устранения недостатков и их последующая профилактика). Он (контур управления) также обеспечивает связь между персоналом управления и всей организацией (предприятием) и повышает эффективность функционирования предприятия в достижении главной цели работы.

Управление – интеллектуальная деятельность, организуя которую в рамках контура управле-

ния информационной безопасностью, реализуются следующие виды (концепции) управленческой деятельности. Первое – научное управление. Оно состоит в повышении эффективности информационной безопасности как составной части производства и включает использование современных методов науки и техники. Здесь главным принципом является специализация, то есть каждый должен делать то, что он делает лучше всего. Второе – административное управление, которое состоит в разработке мероприятий по обеспечению информационной безопасности, исходя из структуры предприятия и особенностей управления производством. Оно включает планирование, организацию и контроль. Третье – управление с позиций психологии и человеческих отношений. Суть состоит в применении приемов управления межличностными отношениями для повышения степени удовлетворенности работников результатами своего труда. Четвертое – управление с позиций науки о поведении, то есть повышение эффективности информационной безопасности как результат использования внутренних человеческих ресурсов. Здесь используются аспекты социального воздействия, мотивации, характера власти и авторитета, коммуникации и лидерства в изменении качества работы и жизни.

Кроме этого, контур управления позволяет реализовывать принципы системного подхода. Это означает, что любой объект анализа рассматривается в качестве системы, состоящей из подсистем. Особое внимание обращается на изучение связей между элементами системы. Исследование исходит из динамической природы любого объекта анализа, а рассмотрение функционирования объекта является результатом его взаимодействия с внешней средой при доминирующей роли в этом процессе внутренних закономерностей объекта. Системный подход подразумевает учет избирательности свойств системы. Это означает, что в данной структуре интегрируются только отдельные из этих свойств, а другим из них должны соответствовать другие структуры.

Таким образом, контур управления информационной безопасностью, как основа менеджмента информационной безопасности, обеспечивает более эффективное управление безопасностью предприятия исходя из складывающихся условий во внутренней и внешней среде.

## ВЫВОДЫ

Контур управления информационной безопасностью предприятия включает в себя мониторинг (сбор, обработку, анализ и систематизацию информации о производственных процессах предприятия и его персонала), моделирование всех возможных сценариев развития событий, разработку на их основе вариантов управленческих решений и после выбора определяющей позиции доведение ее до исполнителей.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Савицкая Г.В. Анализ хозяйственной деятельности предприятия / Г.В. Савицкая. — М.: МГУ, 2010. — 282 с.

2. Шеремет А.Д. Управленческий учет / А.Д. Шеремет. — М.: МГУ, 2010. — 240 с.

3. Лошкарев В.Г. Организация бизнеса с нуля / В.Г. Лошкарев. — М.: Изд-во РИА, 2010. — 204 с.

4. Введение в современную информатику / [М.М. Дивизинюк, Б.С. Бусыгин, Г.М. Коротенко и др.]. — Севастополь: СНУЯЭиП, 2005. — 392 с.

5. Методи керування інформаційною безпекою / [Ю.Ю. Гончаренко, М.М. Дівізінюк, В.О. Хорошко та ин.]. — Севастополь: СНУЯЕтаП, 2010. —328 с.

6. Типизация моделей технологических решений провайдинга Интернет / [М.М. Дивизинюк, Е.В. Азаренко, С.С. Азаров и др. ]. — Севастополь: СНУЯЭиП, 2005. — 112 с.

7. Проектирование систем технической защиты информации / [Ю.Ю. Гончаренко, М.М. Дивизинюк, И.Н. Павлов и др.]. — Севастополь: СНУЯЭиП, 2011. — 235 с.

8. Герасимов Б.М. Системы поддержки принятия решений / Б.М. Герасимов, М.М. Дивизинюк, И.Ю. Субач. — Севастополь: Гос. океанариум, 2004. — 318 с.