Бакаева Жанна Юрьевна
д-р филос. наук, профессор
Холстов Владимир Дмитриевич
аспирант
ФГБОУ ВО «Чувашский государственный университет им. И.Н. Ульянова»
г. Чебоксары, Чувашская Республика

ПРОБЛЕМЫ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *в статье рассматривается проблема эффективного управления компанией. В этом процессе необходимо учитывать бизнес-среду и эталонные модели построения информационной безопасности в контексте эффективности управления компанией. Главное в оценке бизнес-стратегии компании заключается в единстве и проверке данных о подразделениях данной системы. Информационная безопасность является методологией эффективной работы любой компании.*

Ключевые слова: *компания, эффективность, бизнес, риски, стратегические решения, инфраструктура, управление, данные, материальные активы, информационная безопасность.*

Компания, которая профессионально обрабатывает данные – а это немаловажное усилие, – получит взамен выгоды, которые окажутся определяющими в сегодняшней высококонкурентной и постоянно меняющейся среде, такие как:

– принятие стратегических решений;

– более значительные экономические выгоды;

– снижение затрат в различных областях;

– эффективность в маркетинге;

– эффективность операционных процессов;

– улучшение других нематериальных активов (репутацию и т. д.).

И наоборот, неэффективное управление данными может привести к одной или нескольким из проблем. В таких случаях необходимо принять меры, чтобы

предотвратить критическое развитие ситуации и связанные с этим финансовые потери, потери клиентов и/или репутации. Это проблемы:

– данные низкого качества, разрозненные, дублирующиеся, некорректные, устаревшие;

– товар отсутствует на складе или имеется избыток товара;

– недополученная почта из-за неправильно указанных адресов;

– ошибки в выставлении счетов;

– потеря дохода из-за упущенных возможностей;

– неэффективное управление основными данными, препятствующее созданию единого представления;

– невозможность преобразовать эти данные в бизнес-аналитику.

Для решения подобных ситуаций необходимо разработать политику управления данными, которая, независимо от выбора той или иной технологии, должна решать проблему в целом, охватывая все подразделения компании. Реализация плана действий, независимо от конкретных обстоятельств, которые могут подсказать тот или иной подход, будет включать создание автоматически и согласованно управляемого хранилища основных данных. По мере роста объема и сложности этих основных данных будут разрабатываться различные решения для удовлетворения меняющихся требований.

С другой стороны, устранение проблем управления данными требует комплексной системы, реализующей бизнес-стратегию, адаптированную к конкретной компании и основанную на заранее определенных стандартах качества. Ее последующее поддержание, безусловно, предполагает процесс непрерывной проверки записей с конечной целью получения всестороннего представления о бизнесе и использования информации для получения стратегических преимуществ.

На сегодняшний день оценивается недостигшее качественного роста и эффективности в области информатизации, несмотря на масштабные инвестиции, а необходимость управления информационными ресурсами, которая обосновывается признанием таких проблем, как неспособности добиться ощутимых ре-

зультатов, несмотря на увеличение инвестиций, и внутренним скептицизмом в отношении административной эффективности и результативности, достигаемых благодаря информатизации. Во-первых, необходима концептуальная основа для выявления проблем и точной диагностики текущего состояния управления информационными ресурсами, более систематическим и комплексным образом обоснованная. Концептуальная основа (сочетание ключевых элементов и процессов управления информационными ресурсами), способна выявлять проблемы и анализировать текущее состояние управления информационными ресурсами. Во-первых, результаты опроса показали, что низкая эффективность информатизации государственных учреждений за последнее десятилетие в значительной степени объясняется такими факторами, как недостаточное лидерство среди руководителей ведомств, отсутствие сотрудничества между ведомствами и интеграция информационных ресурсов. В результате были определены факторы, требующие дальнейшего улучшения: сотрудничество между ведомствами, роли и обязанности надзорных и координирующих органов, интегрированное управление коммерческими и информационными ресурсами, а также создание системы, ориентированной на результат, наряду с мероприятиями по оценке и совершенствованию. В-третьих, анализ важности ключевых элементов управления информационными ресурсами на каждом этапе процесса показал, что эти элементы сосредоточены в рамках конкретных процессов. Эти выводы позволяют понять текущие проблемы управления информационными ресурсами, предлагают рекомендации для будущего управления и подчеркивают необходимость систематической связи между ключевыми элементами и процессами реализации.

Правительство постоянно инвестирует в информационные системы. Однако результатом этих инвестиций является то, что эффективность не соответствует результатам. Важный момент касается проблем с методом контроля информационной безопасности. Выбор средств контроля информационной безопасности должен осуществляться с учетом результатов оценки рисков информационной безопасности, а метод защиты – то есть метод контроля – может варьиро-

ваться в зависимости от целей и целевых уровней информационной безопасности организации. Средства контроля и методы защиты информационной безопасности должны быть адаптированы к склонности к риску каждой организации, будь то государственные учреждения, крупные корпорации, средние предприятия или малые и средние предприятия. Например, стандартный подход к установке и эксплуатации решений по обеспечению безопасности может оказаться неэффективным против кибератак. Средства контроля информационной безопасности гарантируют снижение риска до приемлемого уровня, а механизм системы информационной безопасности должен основываться на оценке рисков информационной безопасности и принятии риска организацией. Принцип контроля информационной безопасности заключается в проведении анализа рисков и определении необходимых мер контроля на основе результатов обработки рисков. Однако бывают случаи, когда компании ненадлежащим образом применяют эти принципы и стандарты при создании и внедрении системы информационной безопасности. Поэтому при внедрении мер контроля информационной безопасности эффективным подходом может считаться разработка мер информационной безопасности с учетом результатов оценки рисков информационной безопасности. Кроме того, следует помнить, что эффективность информационной безопасности может быть повышена за счет создания и функционирования системы управления, соответствующей организационной среде, посредством управленческих процессов, а не за счет сосредоточения внимания на простых контрольных пунктах или мероприятиях по информационной безопасности, основанных на контрольных списках.

Проблем с подходом и уровнем отечественных систем управления информационной безопасностью, системой управления информационной безопасностью представляет собой структуру и методологию проектирования, внедрения, мониторинга, поддержания и совершенствования.Систематический подход к созданию, внедрению, функционированию, мониторингу, анализу, поддержанию и совершенствованию системы управления информационной безопасностью на основе принципов СУИБ в организации может считаться ключевым фактором

успеха при создании и поддержании системы. Поэтому стратегия создания системы управления информационной безопасностью должна быть реализована на основе принципов информационной безопасности и в соответствии с механизмами информационной безопасности организации. Представляется необходимым рассмотреть механизм информационной безопасности, начиная с создания системы управления информационной безопасностью и заканчивая ее внедрением и поддержкой (с последующим управлением). В частности, анализ проблем корпоративных подходов к системе управления информационной безопасностью с двух точек зрения показывает, что, создание и внедрение системы управления часто оказываются недостаточными с точки зрения «достоверности» и «эффективности»; и, хотя уровень соответствия поддерживается, эффективностью уровней управления и контроля низка [1, с. 34–35].

Проблем с риск-ориентированным подходом к управлению рисками информационной безопасности, следует рассматривать с точки зрения управления рисками информационной безопасности. Внутренние подходы к системе управления информационной безопасностью включают в себя оценку рисков на основе активов (идентификация и оценка активов – угроза – уязвимость – риск – определение целевого состояния – разработка защитных мер; подход к оценке рисков на основе активов). Принципы и рекомендации, которые являются пересмотренной версией метода оценки рисков [1, с. 100–101].

Итак, ключ к управлению рисками в области информационной безопасности заключается в создании процессов идентификации, анализа и оценки рисков. Соответственно, организации должны выбирать и применять средства контроля безопасности, подходящие для уникальной бизнес-среды. Кроме того, желательным подходом является применение стандартов управления рисками, которые могут служить эталонными моделями внутри компании.

Список литературы

1. Константинов С.М. Проблемы современного маркетинга / С.М. Константинов. – М.: Гардарика, 2022. – 230 с.