УДК 658.012.8

РАЗВИТИЕ ПОТЕНЦИАЛА ПОДПРОЦЕССА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

© 2018 Герасимов Б.Н.

Самарский университет государственного управления
«Международный институт рынка», г. Самара, Россия

Управление информационной безопасностью – одна из важнейших частей деятельности любой организации. Определена структура задач управления информационной безопасностью. Разработана технология подпроцесса управления информационной безопасностью организации. Для конкретной организации была разработана совокупность инновационных предложений по улучшению информационной деятельности, а также дан прогноз развития деятельности базовой организации на ближайший период.

Ключевые слова: организация, управление, подпроцессы, информация, безопасность, технологии.

«Как известно, на развитие государства, какой бы формы оно ни было, влияют различные факторы, как внешние, так и внутренние. В современной России крайне важным фактором развития общества и страны в целом является экономический сектор. Это значит, что власть уделяет большую часть своего внимания развитию экономики страны, оперативно реагирует на изменения внутренней и внешней среды, внося изменения во внутреннюю политику» [7].

«Учитывая все экономические и политические события, произошедшие за последние годы, был взят курс на импортозамещение. Из этого следует, что все больше и больше сегодня будет развиваться поддержка отечественного производства. Ярким примером может служить рост поддержки малого и среднего бизнеса со стороны государства» [8].

Но для того чтобы организация жила и развивалась, мало одной лишь поддержки государства. Одна из важнейших целей любого руководителя – эффективное управление организацией. Для квалифицированного управления необходимо доводить все процессы, протекающие в организации, до состояния идеальной слаженности. Часто в организациях проводится реинжиниринг процессов для улучшения общего состояния организации.

В качестве объекта исследования было выбрано ООО «Бигвилл». ООО «Бигвилл» – это крупнейшее самарское интернет-издание, которое существует с 2013 года. На сайте действует несколько разделов, в рамках которых выходят все материалы, как редакционные, так и рекламные. Раздел «News (Новости)» – краткие анонсы городской жизни, событий, мероприятий, гражданских инициатив, статистики. В раздел «Style (Стиль жизни)» входят популярные рубрики «Планы на выходные», «Выходные с детьми», «Новости магазинов», «Новости красоты», Geekvill, тематические гиды. Раздел «City (Город и герои)» – раздел с интервью, «социалкой», материалы о ЖКХ, городских проблемах, медицине. В раздел «Food (Еда)» входит популярная рубрика об общепите, крафтовых и промышленных производителях еды, фермерах. Раздел «Career (Карьера)» – раздел с рубриками «Возможности недели» и «Вакансии недели» о стажировках, грантах, семинарах и вакансиях в Самаре.

В организации существуют три отдела: журналистики, новостной и рекламы. Клиенты ООО «Бигвилл» имеют несколько вариантов коммерческого сотрудничества с изданием.

Во-первых, речь идет об участии в какой-либо рубрике, например в «Новостях красоты». Всего существует 10 рубрик. У некоторых клиентов есть возможность заказать большую статью, например, про то, как устроена их организация изнутри. Такой материал объемом 5000-7000 знаков обязательно сопровождается профессиональной фотосессией. Также в рамках портала у клиентов с

самыми интересными продуктами есть возможность запустить спецпроект, в рамках которого выйдет блок из нескольких статей с возможностью различных тестов, игр и других интерактивов для читателей издания.

Рассмотрим сущность и содержание подпроцесса управления информационной безопасностью в организации.

Информационная безопасность – доступность и конфиденциальность информации, т.е. это состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере [11].

«Управление информационной безопасностью (Information Security Management или ISM) – процесс, который обеспечивает конфиденциальность, целостность и доступность активов, информации, данных и услуг организации. Управление информационной безопасностью обычно является частью организационного подхода к управлению безопасностью организации, который имеет более широкую область охвата, чем поставщик услуг, и включает обработку бумажных документов, доступ в здания, телефонные звонки и тому подобное для всей организации» [10].

Процесс ISM обычно включает в себя следующие подпроцессы:

формирование, управление, распространение и соблюдение политики информационной безопасности и других вспомогательных политик, которые имеют отношение к информационной безопасности организации;

понимание согласованных текущих и будущих требований бизнеса к безопасности организации;

использование контроля безопасности для выполнения политики информационной безопасности организации и управления рисками, связанными с доступом к информации, системам и услугам;

документирование перечня контроля безопасности, действий по их эксплуатации и управлению, а также всех связанных с ними рисков;

контроль всех уязвимостей безопасности и инцидентов, связанных с системами и услугами организации;

проактивное улучшение контроля безопасности и уменьшение рисков нарушения информационной безопасности организации;

интеграция аспектов информационной безопасности во все процессы управления услуг [5].

В ходе анализа ООО «Бигвилл» была выявлена ведущая роль подпроцесса управления информационной безопасностью организации.

Эффективная реализация подпроцесса управления информационной безопасностью предполагает выполнение всех основных функций полного управленческого цикла [4]. К функциям управления в организациях относятся, по работе [4], следующие функции: нормирование; прогнозирование; планирование; организация; учет; контроль; анализ; регулирование; координация. Модель подпроцесса управления информационной безопасностью организации представлена на рисунке 1 [3].

Рисунок 1- Модель подпроцесса управления информационной безопасностью

Полная и своевременная реализация всех функций управления в деятельности организации позволит повысить мобильность и процессность информационной деятельности организации.

В данной организации имеется ряд проблем:

недостаточно серьезный контроль безопасности организации;

недостаточно высокий уровень безопасности в Интернете;

недостаточно высокий уровень безопасности компьютеров и других гаджетов;

недобросовестное отношение рекламодателей к предоставляемой информации организации;

недобросовестное отношение сотрудников к хранению и проверке информации.

Эти и другие проблемы оказывают огромное влияние как на процесс производства, так и на получение предприятием прибыли. В этом случае необходима разработка и внедрение технологии для решения возникших проблем.

Под технологией понимается совокупность методов и процессов, используемых для реализации какой-либо поставленной задачи. Технология предполагает последовательную реализацию следующих этапов: подготовка; проведение; заключительные операции (оформление документации); мониторинг (подведение итогов, их анализ) [2]. Фрагмент технологии управления информационной безопасностью организации представлен на рисунке 2.

На данном этапе работы выделены основные предложения по совершенствованию технологии развития подпроцесса организации. Следует обратить внимание на этап подготовки, в котором описаны основные предложения, которые будут осуществлены в последующих этапах [1].

Для следующего этапа работы необходимо исследовать существующие подпроцессы организации и внедрить инновации в рассматриваемый подпроцесс. Здесь предлагаются элементы, которые нужно усовершенствовать. Этот этап состоит из трех состояний: низкое, нормальное, высокое. Инновационный потенциал подпроцесса управления информационной безопасностью организации управления информационной безопасностью представлен в таблице 1.

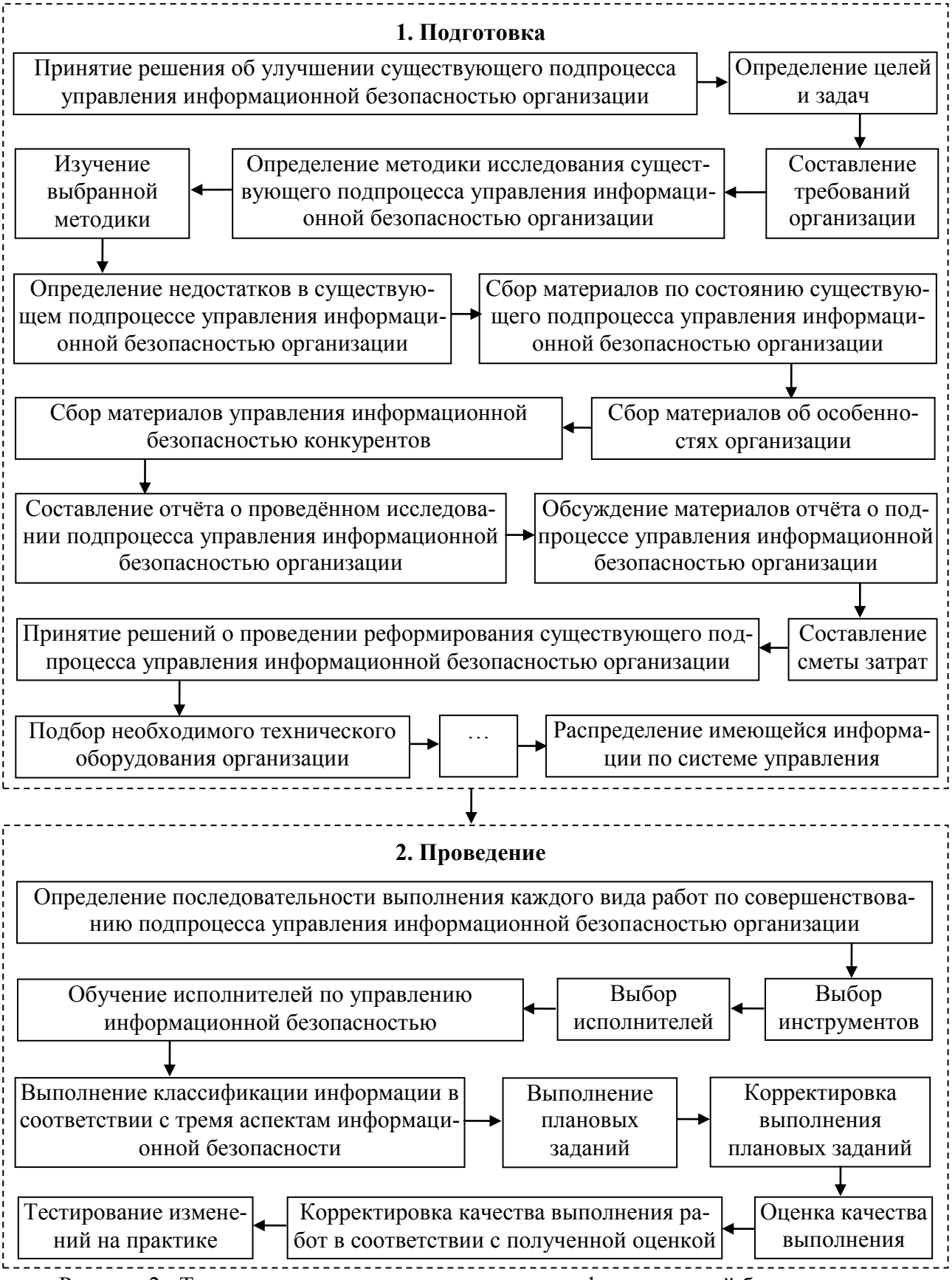

Рисунок 2– Технология подпроцесса управления информационной безопасностью организации (фрагмент)

Таблица 1– Инновационный потенциал подпроцесса управлении информационной безопасностью (фрагмент)

Наименование элемента	Состояние		
	низкое	нормальное	высокое
1. Цели	1.1. Нечеткая формулировка целей. 1.2. Преобладание краткосрочных целей. 1.3. Несоответствие целей требованиям организации	1.1 Преобладание среднесрочных и долгосрочных целей. 1.2 Четкая формулировка целей. 1.3 Закрепление целей в документах организации	1.1 Соответствие целей, миссии, стратегии. 1.2 Полное соответствие целей профилю организации. 1.3 Полное отражение целей в документах организации
2. Задачи	2.1. Нечеткая постановка задач. 2.2. Несоответствие задач целям организации. 2.3. Обобщенная формулировка задач	2.1. Четкая постановка задач. 2.2. Соответствие задач целям организации. 2.3. Разбиение подпроцесса на несколько задач	2.1. Технологизациция задач. 2.2. Отражение целей организации в постановке задач. 2.3. Глубокое структурирование задач организации
3. Ресурсы (технические, трудовые и финансовые)	3.1. Невозможность приобретения технических ресурсов. 3.2. Некачественные трудовые ресурсы в организации (специалисты без опыта работа или должной квалификации). 3.3. Недостаток бюджета для проведения работ	3.1. Приобретение технических ресурсов среднего уровня. 3.2. Средний уровень нанятых специалистов (трудовых ресурсов). 3.3. Обеспечение организации необходимым бюджетом	3.1. Приобретение первоклассных технических ресурсов. 3.2. Привлечение первоклассных специалистов к работе. 3.3. Представление организации большего бюджета для проводимых работ
4. Результаты	4.1. Несоответствие результатов целям. 4.2. Снижение уровня системы управления информационной безопасностью после проводимых работ	4.1. Соответствие результатов целям. 4.2. Поддержание необходимого уровня системы управления информационной безопасностью после проводимых работ	4.1. Результаты, превзошедшие поставленные цели. 4.2. Обеспечение высокого уровня системы управления информационной безопасностью после проводимых работ
5. Специалисты	5.1. Набор сотрудников «по знакомству». 5.2. Отсутствие мероприятий по устранению текучести кадров	5.1 Найм, отбор, адаптация и мотивация сотрудников. 5.2 Планирование и контроль обучения сотрудников	5.1 Оценка личной эффективности сотрудников. 5.2 Регулирование издержек на обучение, обмен опытом

Таким образом, данная организация имеет определенные трудности в проведении инновационного преобразования в рамках организации. Эффективная реализация инновационного потенциала положительно влияет на развитие различных услуг организации. В целом инновационные организации имеют заметно лучшие экономические показатели, чем традиционные [6].

Следующим этапом является разработка инноваций развития подпроцесса управления информационной безопасностью, а затем внедрение и реализация этих предложений для ООО «Бигвилл» (табл. 2).

Таблица 2– Предложения по развитию подпроцесса управления информационной безопасностью организации

Наименование мероприятия	Средства реализации	Ожидаемые результаты
1. Совершенствование целей	1.1. Анализ внутренней среды организации. 1.2. Анализ внешней среды организации. 1.3. Создание группы специалистов для формирования целей.	1.1. Улучшение постановки задач. 1.2. Повышение уровня системы управления информационной безопасностью
2. Совершенствование задач	2.1. Четкая постановка целей. 2.2. Ясные требования компании. 2.3. Работа квалифицированных специалистов над постановкой задач.	2.1 Структурированная работа по управлению информационной безопасностью. 2.2 Повышение уровня системы управления информационной безопасностью
3. Увеличение ресурсов (технических, трудовых и финансовых)	3.1. Привлечение к поиску ресурсов специалистов. 3.2. Поиск дополнительного финансирования. 3.3. Грамотная кадровая политика. 3.4. Приобретение необходимого технического оборудования и обеспечения	3.1. Высокий уровень проводимых работ. 3.2. Повышение уровня системы управления информационной безопасностью. 3.3. Высокий уровень нанятого персонала. 3.4. Высокий уровень технического оснащения
4. Улучшение результатов	4.1. Анализ внутренней среды. 4.2. Анализ внешней среды. 4.3. Анализ итогов проводимых работ. 4.4. Привлечение к анализу полученных данных высококлассных специалистов	4.1 Высокий уровень проводимых работ. 4.2 Повышение уровня системы управления информационной безопасностью. 4.3 Сокращение издержек компании
5. Совершенствование работы с информацией	5.1. Использование всех информационных каналов. 5.2. Проведение полного анализа компании. 5.3. Проведение анализа внешней среды для формирования возможных угроз. 5.4. Привлечение специалистов «со стороны» для проверки информации	5.1 Повышение уровня системы управления информационной безопасностью. 5.2 Повышение репутации организации. 5.3 Повышение конкурентоспособности организации. 5.4 Достоверная информационная база организации

Можно сделать вывод в том, что если организация понесет колоссальные затраты на покупку технического оборудования, персонал и другие виды затрат, то затраты на предложения будут окупаться из-за предоставления дорогостоящих услуг ООО «Бигвилл». Таким образом, каждое из мероприятий по модернизации подпроцесса управления информационной безопасностью имеет определенные условия для начала внедрения изменений.

Рассмотрим экономическое обоснование предложений, т.е. определение основных количественных и качественных экономических показателей, показывающих целесообразность разработки и внедрения технологии и мероприятий.

Эффективность – качественная категория, связанная с интенсивностью развития организации. Она характеризует способность выполнять работу и достигать необходимого или желаемого результата с наименьшей затратой времени и усилий, а также продуктивность использования ресурсов в достижении какой-либо цели.

В ходе исследования в качестве наиболее эффективных мероприятий по улучшению инновационного потенциала организации были выделены следующие:

приобретение необходимого технического оборудования и обеспечения;

привлечение к анализу полученных данных высококлассных специалистов;

профессиональные тренинги для персонала.

Для того чтобы определить целесообразность применения данных предложений, составляется несколько прогнозов деятельности ООО «Бигвилл» [9].

Вначале были представлены сведения о деятельности ООО «Бигвилл». Они были представлены группе экспертов, состоящей из пяти человек. В состав группы экспертов вошли: главный менеджер, менеджер-аналитик, заместители генерального директора по продажам и финансам, а также менеджер-маркетолог.

После проведенного анализа изменения показателей, выполненных экспертами, можно сделать вывод в том, что затраты на сформированные мероприятия принесут организации дополнительный доход, а также положительным образом повлияют на основные экономические показатели ООО «Бигвилл».

Таким образом, на основании проведенной работы можно сделать вывод о том, что подпроцесс управления информационной безопасностью организации включает в себя большое количество ступеней, необходимых для успешной реализации задач в рамках существующих подпроцессов и развития инновационного потенциала. Самое главное в данном подпроцессе – это оказание должного внимания руководством организации, которое не только должно сформулировать политику информационной безопасности организации, но и последовательно обеспечивать необходимые условия для ее реализации.

СПИСОК ИСТОЧНИКОВ

1. Волков О.И. Моделирование и управление бизнес-процессами. Экономика предприятия (фирмы). М.: ИНФРА-М, 2004. 601 с.
2. Герасимов Б.Н. Технологизация процессов в системах управления организации // Вестник Алтайской академии экономики и права. 2015. № 2(40). С. 65-71.
3. Герасимов Б.Н., Чумак В.Г. Социальный менеджмент. Самара: СНЦ РАН, МИР, 2004. 218 с.
4. Герасимов Б.Н. , Чумак В.Г. Проблемно-ситуационные игры в инновационной деятельности организации // Вестник Самарского университета. Аэрокосмическая техника, технологии и машиностроение. 2003. № 2(4). С. 68-75.
5. Егоров А.Ф., Савицкая Т.В. Управление безопасностью химических производств на основе новых информационных технологий. М.: Издательство КолосС, 2004. 416 с.
6. Елизарова О.И. Организация производства и менеджмент. М.: МГУП, 2010.
7. Есипов М.А., Костин Г.А., Курлов В.В. Вычислительные системы, сети и телекоммуникации. СПб.: СПбУТУиЭ, 2011. 196 с.
8. Любушин Н.П., Лещева В.Б., Дьякова В.Г. Анализ финансово-экономической деятельности предприятия. М.: ЮНИТИ-ДАНА, 2004. 121 с.
9. Марцинковский А.В., Данилин В.Н. Управление процессами. Краснодар: Изд-во ГОУВПО «КубГТУ», 2006. 146 с.
10. Соколов Э.М. Информационные технологии в безопасности жизнедеятельности. М.: Машиностроение, 2006. 240с.
11. Хаймович И.Н., Дровянников В.И. Моделирование конкурентного взаимодействия вузов на рынке образовательных услуг // Вестник Самарского государственного экономического университета. 2010. № 1 (63). С. 23-27.

CAPACITY DEVELOPMENT OF SUBPROCESS IN INFORMATION SECURITY MANAGEMENT

© 2018 Boris N. Gerasimov

Samara University of Public Administration «International Market Institute», Samara, Russia

Information security management is one of the most important parts of any organization. The article defines the task structure of information security management. The author developed the technology of subprocess in information security management of the organization. For a specific organization, the author developed a set of innovative proposals to improve information activities, as well as a projected growth of the base organization for the upcoming period.

Keywords: organization, management, subprocesses, information, security, technology