УДК 006.3

ИСПОЛЬЗОВАНИЕ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРАКТИКЕ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ МАЛОГО БИЗНЕСА

ГУСЕЙНОВ Р.И., аспирант ФГУП «СТАНДАРТИНФОРМ»

В статье обоснована необходимость использования международных стандартов информационной безопасности в практике деятельности малых предприятий и разработаны рекомендации по снижению угроз функционированию предприятий малого бизнеса на основе разработки политики информационной безопасности и внедрения соответствующей системы менеджмента.

Ключевые слова: малый бизнес, информационная безопасность, политика информационной безопасности, стандарт.

UDC 006.3

APPLYING INTERNATIONAL STANDARDS IN INFORMATION SECURITY IN THE OPERATIONAL PRACTICE OF SMALL ENTERPRISES

GUSEINOV R.I., post-graduate student at FSUE «STANDARTINFORM»

The article substantiates the necessity of application of international standards of information security in operational practice of small enterprises as well as elaborates recommendations on diminishing the impact of threats to functioning of small enterprises basing on the development of information security policy and introduction of corresponding management system.

Keywords: small business, information security, information security policy, standard.

Практика показывает, что одним из основных видов угроз успешному функционированию и развитию предприятий малого бизнеса в современных условиях являются угрозы информационной безопасности. В этой связи одной из ключевых проблем, стоящих перед руководством малого предприятия, является формирование политики информационной безопасности. Основным требованием к формированию такой политики является возможность реализации предусмотренных в ней мероприятий ограниченным кругом лиц, по-

скольку характерной чертой функционирования малых предприятий является небольшое количество персонала.

При разработке такой политики целесообразно опираться на имеющийся в данной отрасли опыт ведущих мировых производителей. В концентрированном виде этот опыт представлен в стандартах серии ИСО. В связи с этим целесообразно опираться на положения, изложенные в ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности – Требования». Данный ГОСТ идентичен международному стандарту ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements». В рамках данного ГОСТа раскрыто содержание базовых элементов для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности. При этом следует отметить, что принятие решения об инициации разработки остается исключительно за руководителем предприятия, и оно в различной степени будет оказывать влияние на деятельность предприятия на протяжении всего его жизненного цикла. Кроме того, в отсутствии действенной политики в области информационной безопасность риски, связанные с потерей информации и, как следствие, с возникновением финансовых потерь, с течением времени и развития организации будут только возрастать. Таким образом, данное решение имеет стратегический характер.

Поскольку каждое предприятие, в особенности малое, является уникальным, то и система менеджмента будет различной. К основным элементам, оказывающим воздействие на разрабатываемую систему менеджмента, следует отнести:

- потребности организации;
- цели организации;
- требования безопасности;
- используемые процессы;

- масштабы деятельности;
- структура организации.

Отмеченные выше элементы не являются статическими, они обладают изменяющейся природой. Следовательно, менеджмент информационной безопасности, построенный с их учетом, может, с одной стороны, быть изначально адаптированным, с другой – изменяться по мере усложнения элементов. Иначе говоря, для малого предприятия нет необходимости выстраивать систему, используемую в корпорациях, что позволяет в значительной степени сократить использование ресурсов предприятия.

Кроме того, к факторам, детерминирующим целесообразность использования ГОСТ Р ИСО/МЭК 27001-2006, необходимо отнести следующее: выполнение каждого этапа базируется на процессном подходе; в нем представлена модель PDCA (цикл организационного управления, или Цикл Деминга – Шухарта): «Планирование (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (PDCA); он гармонизирован с другими ведущими международными стандартами. Модель применима в различных условиях вне зависимости от размера, характера и рода деятельности организации. Кроме того, она поддается модификации в зависимости от целевых задач ее использования. Данная модель представлена на рис. 1.

Модель PDCA также отражает принципы, установленные в Директивах Организации экономического сотрудничества и развития (ОЭСР) и определяющие безопасность информационных систем и сетей [1].

ГОСТ Р ИСО/МЭК 27001-2006 гармонизирован с ИСО 9001:2000 «Системы менеджмента качества. Требования» и ИСО 14001:2004 «Системы управления окружающей средой. Требования и руководство по применению», что позволяет исключить противоречия при ее интеграции с иными системами менеджмента.

В результате практического внедрения данной модели малое предприятие формирует политику в области информационной безопасности, которая полностью отвечает его насущным потребностям и учитывает его особенно-

сти, данная политика приобретает формализованный вид и может быть оформлена в качестве одного из базовых документа предприятия. Далее на малом предприятии появляется персонал, обладающий необходимым уровнем знаний в области информационной безопасности, кроме того, ряд сотрудников становится способным развить свою компетенцию проведения процедур, позволяющих минимизировать возможные неблагоприятные последствия в случае серьезного инцидента (например, несанкционированного проникновения (атаки хакеров) на веб-сайт организации).

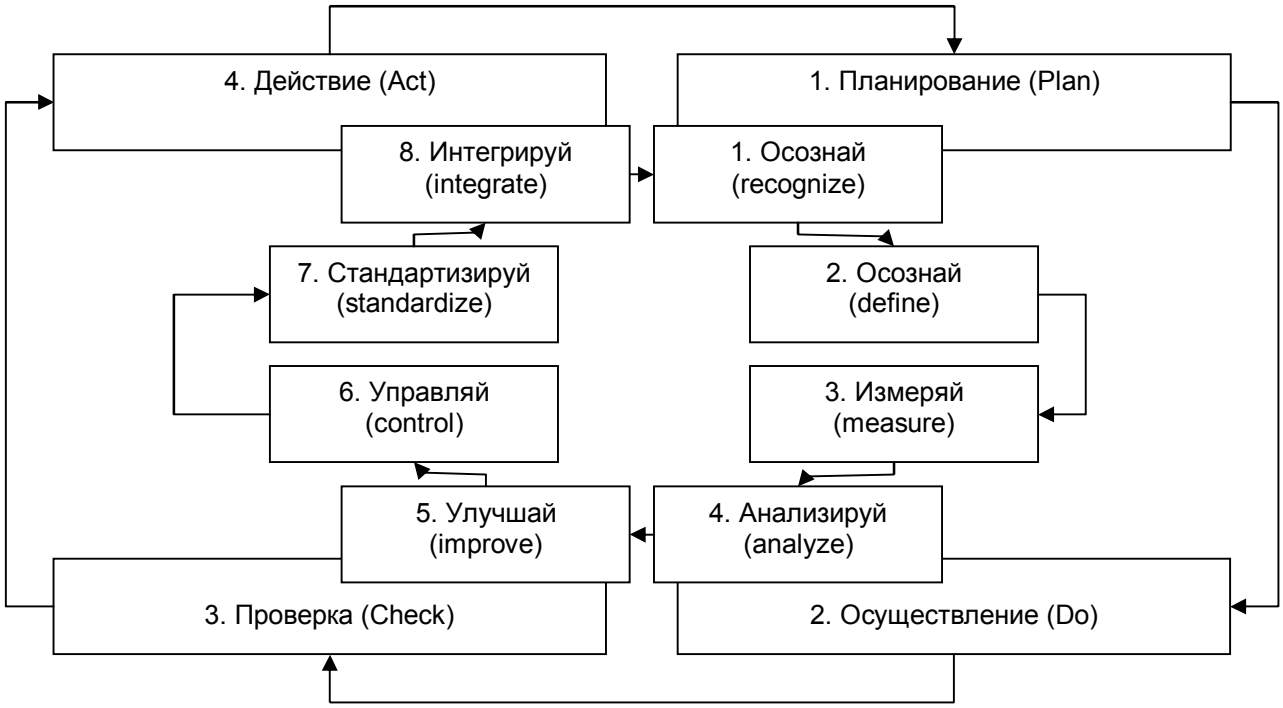

Рис. 1. Модель PDCA и ее модификация

Следует отметить, что понятие «информационная безопасность» имеет достаточно большое количество трактовок, приведем лишь некоторые из них, которые наиболее распространены.

Информационная безопасность – защищенность жизненно важных интересов личности, общества и государства от преднамеренных или непреднамеренных воздействий в той или иной форме (информационная блокада, информационная интервенция, информационная война, дезинформация и

др.); обеспечение сохранности информационных ресурсов государства и защищенность законных прав личности и общества в сфере информации [2].

Информационная безопасность (по законодательству РФ) – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства [3].

Безопасность информационная – состояние, обеспечивающее защищенность информационных ресурсов и каналов, а также доступа к источникам информации [4].

По мнению автора, в качестве основы целесообразно использовать определение, закрепленное в стандарте. Под информационной безопасностью (ИБ) (information security) будем понимать свойство информации сохранять конфиденциальность, целостность и доступность, аутентичность, подотчетность, неотказуемость и надежность. Применительно к малому предприятию особое значение имеет такое свойство информации, как аутентичность и надежность [5]. Данные свойства тесным образом связаны с понятием менеджмента риска.

Менеджмент риска (risk management) – скоординированные действия по руководству и управлению организацией в отношении риска, которые включают в себя оценку риска, обработку риска, принятие риска и коммуникацию риска [6].

Определим также, что инцидент информационной безопасности (information security incident) – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность [7]. Инцидентами информационной безопасности являются:

1) утрата услуг, оборудования или устройств;
2) системные сбои или перегрузки;
3) ошибки пользователей;
4) несоблюдение политики или рекомендаций по ИБ;
5) нарушение физических мер защиты;

6) неконтролируемые изменения систем;

7) сбои программного обеспечения и отказы технических средств;

8) нарушение правил доступа.

При этом следует отметить, что четвертый пункт «несоблюдение политики или рекомендаций по ИБ» является комплексным и по своей сути в нем в различной степени содержится весь приведенный перечень. С другой стороны, исходя из данных, приведенных на рисунке 2, такие меры обеспечения информационной безопасности, как проведение политики ИБ в различных ее направлениях, использует относительно небольшое число организаций малого бизнеса.

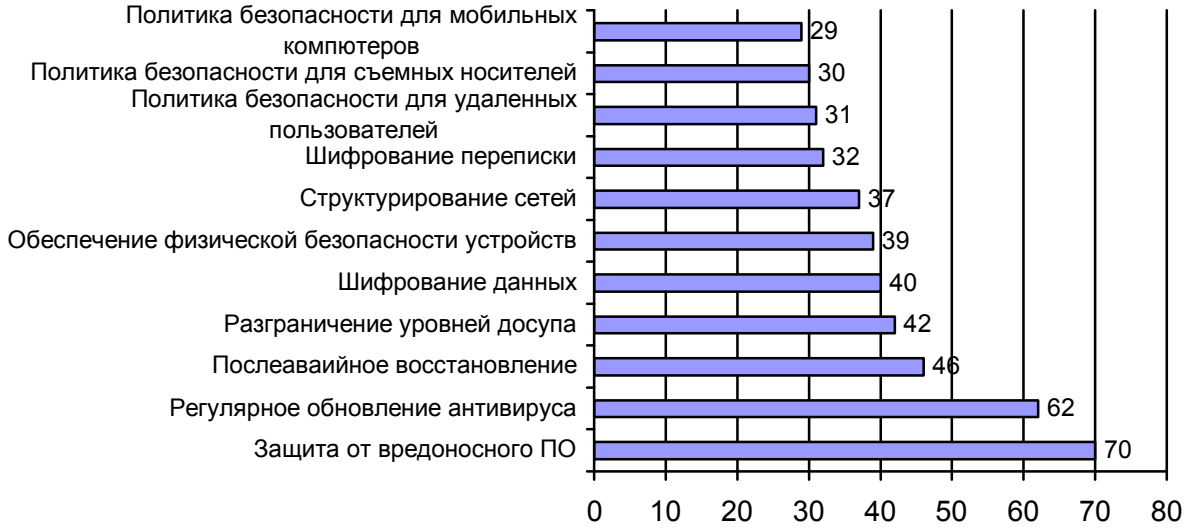

Рис. 2. Наиболее распространенные меры обеспечения информационной безопасности на предприятиях малого бизнеса [8]

Исходя из сказанного выше, разработка системы менеджмента информационной безопасности малого предприятия на основе положений ГОСТ Р ИСО/МЭК 27001-2006 и с учетом особенностей функционирования данного предприятия, является одним из ключевых элементов его деятельности.

В ходе осуществления разработки необходимо обратить внимание на следующие элементы.

1. Выделить область применения системы. Поскольку малое предприятие в своей деятельности использует также небольшое количество техниче-

ских средств, то существуют основания для изначального применения системы во всех сферах деятельности организации.

2. Сформировать политику информационной безопасности, включающую:

- цели реализации системы менеджмента;
- направления реализации;
- характер действий;
- взгляды руководства на информационную безопасность;
- определить критерии оценки ИБ.

Указанные составляющие политики информационной безопасности должны определяться с учетом требований осуществления деятельности на конкретном рынке и действующего законодательства. Также необходимо отметить, что разрабатываемая политика должна быть гармонизирована с общей стратегией развития организации. Поскольку существует значительная доля вероятности того, что разработанная политика и система информационной безопасности могут лечь в основу управления рисками организации, то базовые общетеоретические положения политики целесообразно представить в виде концепции. Концепция – (от лат. conceptio – понимание, система) – определенный способ понимания, трактовки какого-либо предмета, явления, процесса; основная точка зрения на предмет или явление, руководящая идея для их систематического освещения; ведущий замысел, конструктивный принцип в научной, художественной, технической, политической и других видах деятельности [9]. Естественно, что она должна быть всецело поддержана руководством организации.

При определении критериев оценки информационной безопасности и риска возникновения инцидентов необходимо: определить методологию оценки риска; разработать критерии принятия риска и определить приемлемые уровни риска. При определении методологии определения риска целесообразно обратиться к ИСО/МЭК ТО 13335-3:1998 «Руководство по управлению безопасностью информационных технологий. Часть 3. Методы управле-

ния безопасностью информационных технологий», где приведены различные примеры практического использования различных методологий.

Для установления рисков необходимо [10]:

- определить средства, задействованные в бизнес-процессах, где планируется реализация системы менеджмента;
- определить конкретных пользователей средств коммуникации и информационными базами данных;
- установить перечень возможных угроз применительно к данным средствам;
- установить слабые места перечисленных средств, которые могут привести к нарушению безопасности [11];
- определить возможные последствия при наступлении инцидента на различных этапах реализации бизнес-процесса.

При анализе выявленных либо предполагаемых рисков целесообразно:

- определить вред, наносимый организации в результате возникновения инцидента;
- определить уровни риска;
- осуществить коррекцию процессов либо их отдельных этапов с целью ликвидации недопустимого уровня риска.

К уровням риска следует отнести количественные и качественные значения рисков для обозначения степени опасностей и угроз безопасности человека, объектов техносферы и окружающей среды. К качественным характеристикам уровней риска относятся – пренебрежимые, приемлемые, допустимые, неприемлемые, чрезмерные, недопустимые. При количественном определении уровней риска используются различные шкалы риска, устанавливаемые при анализе риска. Указанным выше качественным уровням риска соответствуют определенные граничные количественные значения уровней; для индивидуальных рисков логарифмическая шкала уровней риска устанавливается в виде математического ожидания ущерба в единицу времени [12].

В ходе осуществления коррекции бизнес-процессов либо их отдельных этапов с целью ликвидации недопустимого уровня риска возможно проведение менеджментом организации различного рода мероприятий. После этого необходимо самоопределение руководства организации в отношении возможности осуществления бизнес-процессов при данном уровне риска.

Следует также отметить, что необходимо проанализировать возможность передачи ряда процессов, связанных с риском, сторонним организациям. Отмеченная передача может быть в полной мере осуществлена и предприятиями малого бизнеса. Например, Государственное бюджетное учреждение «Малый бизнес Москвы» (МБМ), осуществляющее свою деятельность при содействии Департамента науки, промышленной политики и предпринимательства города Москвы, предлагает информационную поддержку и сопровождение малого бизнеса.

Данное предприятие осуществляет поддержку в организации и проведении торгово-выставочной деятельности. Выставки для малого бизнеса являются весьма эффективным способом распространения информации о производимой продукции, предлагаемых услугах и об организации в целом. Они являются местом пересечения интересов различных сторон: конечных покупателей; посредников; производителей. Также малым предприятиям предоставляется возможность для: изучения рынка; исследования деятельности ведущих производителей отрасли; определения тенденций на рынке.

Одним из существенных препятствий участия малых предприятий в выставочных мероприятиях является значительный финансовый порог, т.е. совокупность финансовых затрат на аренду площадей, оформление выставочного места, хранение продукции и т.д. МБМ совместно с Департаментом науки, промышленной политики и предпринимательства города Москвы предлагает минимизировать указанные расходы. Малые и средние предприятия могут рассчитывать на получение субсидии до 250 000 рублей для участия в зарубежных и отечественных выставках, ярмарках и конференциях – до 2/3 затрат на участие в мероприятиях [13].

Исходя из вышеизложенного, можно сделать следующее заключение. К основным причинам возникновения повышенного уровня риска информационной безопасности малого бизнеса следует отнести: а) минимальный уровень ресурсообеспечения; б) недостаточный уровень знаний, умений и навыков в области основ обеспечения информационной безопасности; в) низкий уровень информированности об информационных угрозах и их последствий для ведения бизнеса.

В этой связи предприятиям малого бизнеса целесообразно использовать соответствующие международные стандарты, на основе которых необходимо внедрение систем менеджмента информационной безопасности.

Список использованной литературы

1. OECD, Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. Paris: OECD, July 2002. – www.oecd.org.
2. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / Автор-составитель В.Ф. Пилипенко. – Изд. 2-е, доп. и перераб. – М.: ПЕРСЭ-Пресс, 2005.
3. http://dic.academic.ru/dic.nsf/fin_enc/23419.
4. http://voina-i-mir.ru/dicdefinition/?id=32.
5. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности – Требования».
6. Руководство ИСО/МЭК 73:2002 «Управление риском. Словарь. Руководящие указания по использованию в стандартах».
7. ИСО/МЭК ТО 18044:2004 «Информационная технология – Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
8. http://www.kaspersky.ru/.
9. Философский энциклопедический словарь // Гл. редакция: Л.Ф. Ильичёв, П.Н. Федосеев, С.М. Ковалёв, В.Г. Панов. – М.: Советская энциклопедия, 1983.
10. ИСО/МЭК ТО 13335-3:1998 «Руководство по управлению безопасностью информационных технологий. Часть 3. Методы управления безопасностью информационных технологий».
11. http://glossary.ru.
12. EdwART. Словарь терминов МЧС, 2010 http://dic.academic.ru/dic.nsf/emergency/.
13. http://www.mbm.ru/market/beginner/participation-in-exhibitions-and-fairs/.