УДК 004.056.5

РАЗРАБОТКА И ВНЕДРЕНИЕ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ISO/IEC 27001:2013

Хвистик М.Д., Серенков П.С.

Белорусский национальный технический университет
Минск, Республика Беларусь

Аннотация. Рассмотрена информация как один из важнейших ресурсов в жизни современного человека и необходимость ее защиты. Была проанализирована актуальность разработки и внедрения системы менеджмента информационной безопасности в ИТ-компаниях. Также была проанализирована необходимость получения сертификата соответствия ISO/IEC 27001:2013.
Ключевые слова: информация, СМИБ, Confluence, сертификат, ISO/IEC 27001:2013.

DEVELOPMENT AND IMPLEMENTATION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM IN ACCORDANCE WITH ISO/IEC 27001:2013

Khvistik M., Serenkov P.

Belarusian National Technical University
Minsk, Belarus

Abstract. Information was considered as one of the most important resources in the life of a modern person and the need to protect it. The relevance of the development and implementation of an information security management system in IT companies was analyzed. The necessity of obtaining a certificate of compliance with ISO/IEC 27001:2013 was also analyzed.
Key words: information, ISMS, Confluence, certificate, ISO/IEC 27001:2013.

Адрес для переписки: Хвистик М.Д., пр. Независимости, 65, г. Минск 220113, Республика Беларусь
e-mail: mkhvistikm@gmail.com

Информация – сведения, независимо от формы их представления, воспринимаемые человеком или специальными устройствами как отражение фактов материального мира в процессе коммуникации. Нет смысла спорить, что в 21 веке информация – один из важнейших ресурсов в жизни человечества.

На первый план в современном обществе выходит проблема информационной безопасности практически во всех отраслях деятельности человека. В ИТ-сфере потеря информации является одной из ключевых проблем: потеря баз данных, результатов аналитических исследований, исходных кодов, программных продуктов, персональных данных клиентов означает угрозу для продолжения бизнеса. *Медицинские организации являются операторами персональных данных пациентов. Они принимают участие в сборе, систематизации, накоплении, хранении, уточнении, обновлении, изменении, распространении и уничтожении такой информации.* В банковской отрасли могут быть случаи утечки баз данных, содержащих персональные данные субъектов, а также участившиеся случаи несанкционированной передачи персональных данных со стороны финансовых организаций третьим лицам.

В связи с необходимостью защиты информации белорусские компании разрабатывают и внедряют систему менеджмента информационной безопасности в соответствии с СТБ ISO/IEC 27001 или в соответствии с ISO/IEC 27001, если компания ориентируется на международный рынок.

Компания выбирает необходимые меры управления безопасностью, предназначенные для защиты информационных активов и гарантирующие доверие заинтересованных сторон. В соответствии с международным стандартом информационная безопасность трактуется как сохранение конфиденциальности, доступности и целостности информации, достичь этого можно с помощью управления рисками. На этом и базируется стандарт ISO/IEC 27001:2013 [1].

Компания ООО «Эффективные программы», позиционирующая себя как разработчик программной продукции для организаций широкого профиля деятельности заинтересована в разработке и внедрении системы менеджмента информационной безопасности. Причина – требования рынка. Высокая конкуренция заставляет демонстрировать ИТ – компаниям широкий спектр возможностей для обеспечения высокой степени удовлетворенности потребителя.

Отличительной особенностью разработки СМИБ в данной компании, является то, что вся документация СМИБ была разработана и находится на электронном ресурсе Confluence вики-системе для внутреннего пользования Компанией. Что в ходе сертификационного аудита, было отмечено аудиторами, как явный показатель прогресса и удобства в использовании.

Цели управления и средства управления из приложения А стандарта ISO/IEC 27001 должны быть выбраны как часть этого СМИБ-процесса для того, чтобы удовлетворять определенные требования. Цели управления и средства управления, перечисленные в приложении А стандарта ISO/IEC 27001, получены непосредственно из перечня целей управления и средств управления,

перечисленных в разделах 5–15 ISO/IEC 17799:2005, и согласованы с ними [2].

Следует отметить, что эффективное и результативное внедрение СМИБ возможно только учитывая принципы процессного подхода, в соответствии с ISO 9001:2015. Цель такой модели – выявить источники появления рисков и места их возникновения, что позволяет построить процессы таким образом, чтобы локализовать источники или вовсе их устранить.

Процессный подход, представленный в семействе стандартов СМИБ, основан на операционном принципе, принятом в стандартах ISO на системы управления, и известном как процесс «План (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (цикл PDCA) [2].

В связи с этим, перед тем, как приступить к разработке системы, в компании были проанализированы существующие процессы на предмет возможных угроз и присущих уязвимостей. Была просчитана вероятность возникновения рисков и методы управления ими.

Далее разработка системы менеджмента информационной безопасности велась по плану действий, который можно визуализировать с помощью диаграммы Ганта (рис.1). Следует отметить, что в данном плане указаны только ключевые этапы, без детального описания.

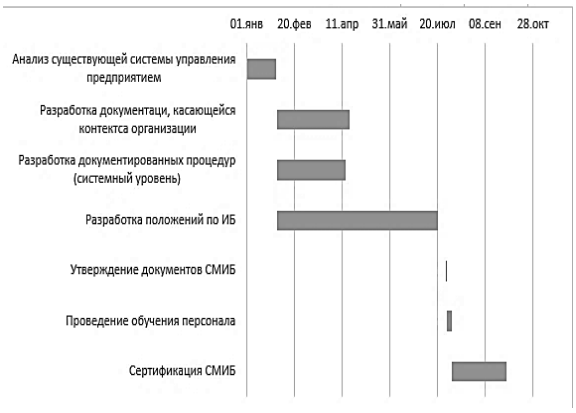

Рисунок 1 – План действий «Разработки документации системы менеджмента информационной безопасности, соответствующей ISO/IEC 27001»

В соответствии с планом, приведенным выше, на первом этапе велись работы по распределению ответственности, актуализации должностных инструкций, разработке актуальной организационной структуры и органиграммы, а также по планированию системы и по организационной деятельности.

Разработка документации, касающейся контекста организации, включала в себя проведение SWOT-анализа метом мозгового штурма, оформление протокола анализа и мониторинга. Протокол стал основой для составления контекста организации и определения рисков деятельности организации.

Третий этап – разработка документированных процедур, включал в себя формальное описание таких процессов в компании, как: менеджмент рисков, управление документированной информацией, менеджмент непрерывности бизнеса и других, а также формирования фонда НПА и НД и Глоссария.

Этап разработки положений по информационной безопасности являлся самым длительным, так как состоял из подготовки частных политик, которые были разработаны в соответствии с Приложением А стандарта ISO/IEC 27001, и формирования Заявления о применимости (SoA).

Проведение обучения сотрудников компании включало в себя ознакомление персонала с документированной информацией СМИБ, файлом с аудио-обучением посредством отправки по корпоративной электронной почте ссылки и коммуникациями в Skype непосредственно перед проведением сертификационного аудита. Сотрудники под роспись были ознакомлены с приказами руководства, документированной информацией и файлом с обучением по ISO/IEC 27001.

Соответствие рабочих процессов компании описанным политикам было подтверждено при проведении внутренних аудитов.

Таким образом, компания была готова к сертификации в 2021 году. Этап «Сертификация СМИБ», включал в себя: подготовку отчетных документов необходимых для прохождения сертификационного аудита, формирование и подачу заявки в орган по сертификации, прохождение первого этапа сертификационного аудита, работу над несоответствиями и аспектами для улучшения, выявленными на первом этапе сертификационного аудита и прохождение второго этапа сертификационного аудита.

На данный момент компания находится в ожидании получения сертификата на соответствие ISO/IEC 27001.

Прохождение сертификации много значит для компании, так как сертификат обеспечивает доверие заказчиков, гарантирует защиту персональных данных клиентов и дает конкурентное преимущество на рынке.

Литература

1. ISO/IEC 27001 [Электронный ресурс]: Википедия. Свободная энциклопедия. – Режим доступа https://ru.wikipedia.org/wiki/ISO/IEC_27001. – Дата обращения: 19.09.2021.

2. ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary [Электронный ресурс]. – Режим доступа https://ru.wikipedia.org. – Дата обращения: 19.09.2021.