УДК 004.056

ПОДХОДЫ К РАЗРАБОТКЕ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ ОРГАНИЗАЦИЯХ В КОНТЕКСТЕ КОНЦЕПЦИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

В.А. Бойправ, Л.Л. Утин

В Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 09.11.2010 г. № 575, определено, что одной из составляющих национальной безопасности является информационная безопасность, которая представляет собой состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

В данном документе классифицированы все основные угрозы в информационной сфере. Как минимум 5 из 15 видов угроз в информационной сфере можно отнести непосредственно к деятельности телекоммуникационных организаций.

Основными внутренними источниками угроз являются:

- недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;
- рост преступности с использованием информационно-коммуникационных технологий;
- несовершенство системы обеспечения безопасности критически важных объектов информатизации.

Основными внешним источниками угроз являются:

- открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;
- попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь [2].

Учитывая темпы развития информационно-телекоммуникационных (ИТК) технологий и увеличение скорости передачи информации, можно прогнозировать рост потенциального ущерба от реализации этих угроз в информационной сфере.

С целью недопущения нанесения ущерба (снижения последствий от реализации угроз) в ИТК, телекоммуникационным организациям необходимо создавать системы обеспечения информационной безопасности. Одним из наиболее эффективных способов обеспечения безопасности в информационной сфере, является построение системы менеджмента информационной безопасности (СМИБ). Как правило, построение таких систем осуществляется в соответствии с международными стандартами семейства ISO/IEC 27000.

Согласно данным Международной организации по стандартизации, в 2014 году в мире было выдано и действовало 23 972 сертификата, удостоверяющих соответствие применяемых на предприятиях СМИБ требованиям стандарта

ISO/IEC 27001 (рост 7 % к уровню 2013 года, при общем росте количества выданных сертификатов на 3 %) [4].

Несмотря на рост популярности СМИБ во всем мире, в Республике Беларусь в течение пяти прошедших лет только одна организация сертифицировала свою систему менеджмента информационной безопасности на соответствие требованиям СТБ ISO/IEC 27001-2011 в Национальной системе подтверждения соответствия Республики Беларусь. Отсутствие сертифицированных СМИБ у всех операторов связи Республики Беларусь также можно отнести к внутренней угрозе ИБ.

Наметившаяся тенденция роста инцидентов в области ИБ делает актуальным исследование вопросов создания и повышения эффективности СМИБ.

При рассмотрении вопросов в информационной сфере и в области ИБ необходимо использовать основные термины, определенные в Законе Республики Беларусь «Об информации, информатизации и защите информации», а также руководствоваться действующими в Республике Беларусь государственными стандартами в области информационной безопасности, являющимися аналогичными международным стандартам ISO/IEC серии 27000. В данных документах определены базовые мероприятия по обеспечению защиты информации, направленные на обеспечение ее конфиденциальности, целостности, подлинности, доступности и сохранности.

Как показывает анализ, руководство телекоммуникационных организаций уделяет недостаточно внимания вопросам информационной безопасности. В сети Интернет можно найти сведения об абонентах практически всех крупных телекоммуникационных сетей. Получить любые другие персональные сведения абонентов ИТК сетей (продолжительность разговоров, данные об исходящих и входящих сообщениях, перемещение в течение суток и т.д.) через иные источники не составляет большого труда. Это является прямым нарушением статьи 28 Конституции Республики Беларусь, согласно которой каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство [1]. Доступность персональных сведений способствует росту преступлений с использованием информационно-коммуникационных технологий.

Рассматривая вопросы безопасности в информационной сфере, необходимо выделить в отдельную задачу обеспечение устойчивого функционирования критической отраслевой инфраструктуры (КОИ) и критически важных объектов информатизации (КВОИ). Несмотря на то, что эта функция возложена на соответствующие органы государственного управления, руководству телекоммуникационных организаций целесообразно самостоятельно рассмотреть это вопрос с учетом требований Концепции национальной безопасности. Необходимо определить перечень КОИ и КВОИ, решить, при необходимости, организационно-правовые вопросы выделения их в отдельные организации (структурные подразделения) и разработать комплекс

мероприятий по их эффективной защите и обеспечению непрерывного функционированию [5].

Разработка, внедрение и сертификация системы менеджмента ИБ по СТБ 27001-2011 позволяет реализовать телекоммуникационным организациям следующее:

- структурировать информационные активы;
- определить основные угрозы безопасности в существующих производственных процессах;
- идентифицировать риски и управлять ими;
- нацеливать персонал организации на постоянное совершенствование ИБ с учетом развития технологий, методов и влияния конкурентной среды;
- эффективно управлять ИТК сетями в критических ситуациях для минимизации ущерба [3].

Не подвергая ревизии значимость и практическую ценность рекомендаций, изложенных в стандартах ISO/IEC серии 27000, следует признать, что изложенные в них положения не всегда соответствуют национальным интересам и требованиям законодательства Республики Беларусь. Следовательно, построение СМИБ только на основе настоящих рекомендаций не приведет к существенному снижению потенциального ущерба от угроз в сфере информационной безопасности Республики Беларусь, т.к. при этом будут применяться широко известные и активно распространяемые алгоритмы защиты данных. Все вышеуказанное позволяет сделать вывод о том, что при разработке СМИБ в телекоммуникационных организациях на основе рекомендаций национальных и международных стандартов ISO/IEC серии 27000, необходимо дополнительно использовать собственные (не стандартизированные) методы, основанные на требованиях Концепции национальной безопасности Республики Беларусь. Использование предложенного комплексного подхода при разработке СМИБ в телекоммуникационных организациях будет способствовать решению задачи защиты национальных интересов Республики Беларусь в информационной сфере.

Список использованных источников

1. Конституция Республики Беларусь (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г. и 17 октября 2004 г.). – Минск: Амалфея, 2005. – 48 с.

2. Об утверждении концепции национальной безопасности Республики Беларусь: Указ Президента Респ. Беларусь, 9 ноября 2010 г., № 575// Консультант Плюс : Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2012.

3. Бойправ, В.А. Проведение аудита системы информационной безопасности на предприятии отрасли связи // В.А. Бойправ, О.В. Бойправ, Л.М. Лыньков / Управление информационными ресурсами: матер. IX Междунар. науч.-практ. конф., Минск, 21 ноя. 2012 г. / редкол. А.В. Ивановский [и др.]. – Минск: Акад. Упр. При Президенте Респ. Беларусь,

2012. – С. 69 – 70.

4. Бойправ, В.А. Методика обеспечения информационной безопасности на предприятии отрасли связи // В.А. Бойправ, О.В. Бойправ, Л.М. Лыньков / Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: матер. Междунар. науч.-техн. сем. Минск, янв.–дек., 2012 г. / редкол. М.Н. Бобов [и др.]. – Минск: БГУИР, 2012. – С. 83–86.

4. The ISO Survey of Management System Standard Certifications – 2014. – [Электронный ресурс]. – 2014. – Режим доступа: http://www.iso.org/iso/ru/iso_survey_executive-summary.pdf?v2014. – Дата доступа: 10.03.2016 г.

5. Перевалов, Д.И. Методологические и правовые аспекты формирования системы критически важных объектов и обеспечения ее безопасного функционирования / Д.И. Перевалов // Право.by. – 2014. – № 5(31).– С. 75–79.

Бойправ Владимир Андреевич, аспирант БГУИР, name_abs@rambler.ru

Утин Леонид Львович, начальник кафедры связи военного факультета Белорусского государственного университета информатики и радиоэлектроники, кандидат технических наук, доцент, ullktn@mail.ru