

ПРИНЦИПЫ РЕАЛИЗАЦИИ МЕТОДИКИ АУДИТА СИСТЕМЫ МЕНЕДЖМЕНТА ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИЯХ ЭЛЕКТРОСВЯЗИ

В.А. БОЙПРАВ, Л.Л. УТИН

*Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь*

Поступила в редакцию 30 июня 2016

Выполнена оценка специфики деятельности организаций электросвязи Республики Беларусь. С использованием результатов этой оценки, а также с учетом требований нормативных и правовых актов Республики Беларусь в областях защиты информации и электросвязи обоснованы принципы реализации методики аудита системы менеджмента защиты информации в таких организациях.

Ключевые слова: аудит, организация электросвязи, система менеджмента, защита информации.

Введение и постановка задач

В Республике Беларусь с каждым годом увеличивается удельный вес организаций, использующих в своей деятельности сети электросвязи для получения и предоставления информации, обмена официальными документами. Это подтверждается соответствующими статистическими данными (рис. 1, 2) [1].

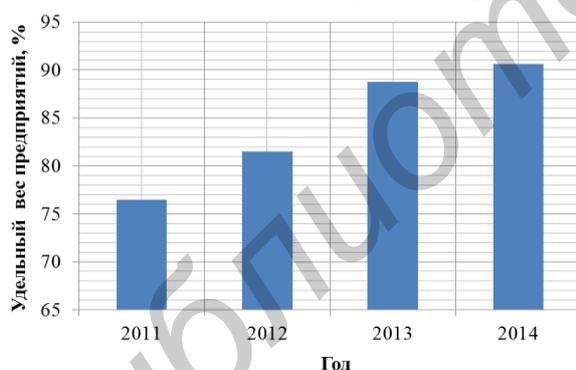


Рис. 1. Динамика удельного веса организаций Республики Беларусь, использующих сети электросвязи для получения и предоставления информации, в общем количестве организаций за период 2011–2014 гг.

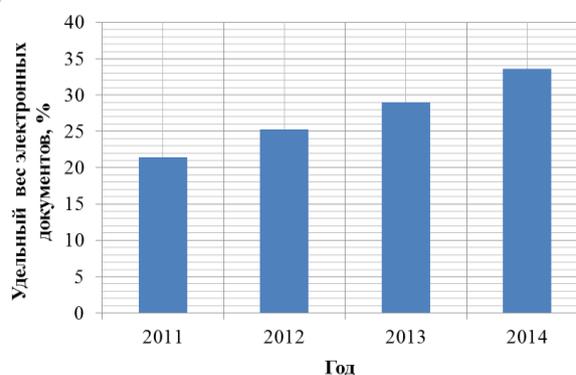


Рис. 2. Динамика удельного веса электронных официальных документов в общем количестве документов за период 2011–2014 гг.

На основе результатов анализа статистических данных, представленных на рис. 1, 2, можно сделать вывод о том, что в течение прошедшей пятилетки в Республике Беларусь наблюдалось увеличение в среднем на 5 % в год количества организаций, использующих сети электросвязи в своей повседневной деятельности (оптовый и розничный товарооборот, получение заказов на оказание услуг, электронный документооборот и т.п.). Кроме того, в течение названного промежутка времени увеличивался в среднем на 3 % в год объем официальных документов, представляемых и передаваемых в электронном виде. Таким образом, можно сделать вывод о том, что в Республике Беларусь с каждым годом возрастает количество организаций, эффективность функционирования и объем прибыли которых зависят

от полноты выполнения организациями электросвязи своих обязанностей, перечень которых определен в Законе Республики Беларусь от 19 июля 2005 г. № 45-З «Об электросвязи». Согласно положениям названного закона, организации электросвязи должны обеспечивать своевременность и качество предоставления потребителям своей продукции (т.е. услуг электросвязи) в соответствии с обязательными для соблюдения требованиями технических нормативных правовых актов в области технического нормирования и стандартизации [1].

Установлено, что в настоящее время сфера услуг электросвязи является одной из наиболее привлекательных для инвестирования в экономике Республики Беларусь (рис. 3) [1].

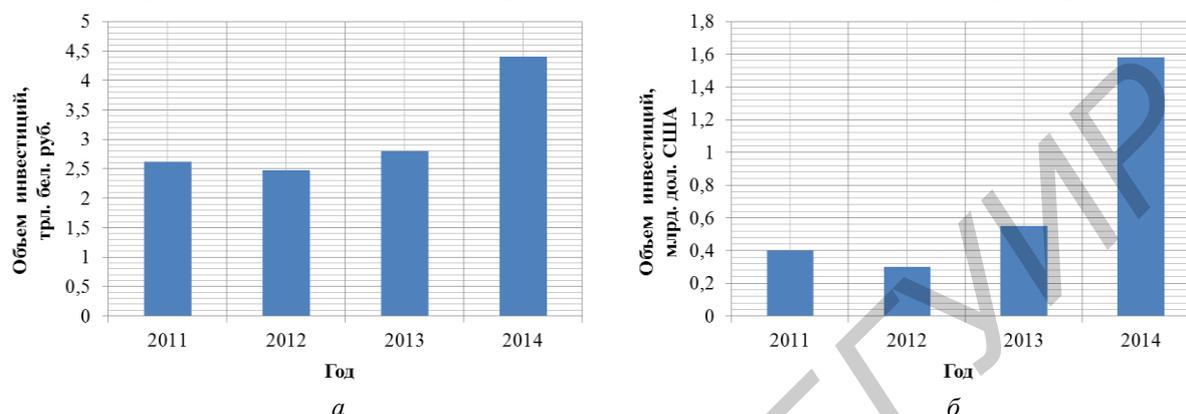


Рис. 3. Динамика объема инвестиций, поступивших в сферу услуг электросвязи Республики Беларусь за период 2011–2014 гг.: а – общий объем инвестиций; б – объем иностранных инвестиций

В течение 2011–2014 гг. в Республике Беларусь наблюдался рост окупаемости инвестиций в сферу услуг электросвязи, что способствовало уменьшению с 17,7 до 7,6 % удельного веса убыточных организаций электросвязи в общем количестве организаций. Одним из важных способов обеспечения положительной динамики рассмотренных параметров является совершенствование системы менеджмента на предприятиях электросвязи. Обязательной составляющей системы менеджмента организации электросвязи должна быть система менеджмента защиты информации (СМЗИ).

Многообразие и имеющаяся противоречивость требований международных стандартов, национальных нормативных и правовых актов в области защиты информации приводит к недостаточно четкому пониманию различными организациями принципов, в соответствии с которыми в этих организациях может быть проведен аудит СМЗИ.

В рамках настоящей статьи для формирования принципов проведения аудита СМЗИ в организациях электросвязи Республики Беларусь были решены следующие задачи:

1) проведен анализ нормативных и правовых актов, регламентирующих деятельность организаций электросвязи Республики Беларусь, а также осуществлена оценка специфики этой деятельности;

2) выполнен обзор стандартов, используемых для проведения аудита системы менеджмента защиты информации на предприятиях, и установлены его принципы.

Специфика деятельности организаций электросвязи в Республике Беларусь

В Республике Беларусь деятельность организаций электросвязи, независимо от их форм собственности и индивидуальных предпринимателей, работающих в области электросвязи, регулируется Министерством связи и информатизации [2, 3]. В его состав входят 13 организаций (из них коммерческих государственной формы собственности – 5, финансируемых из бюджета – 2, открытых акционерных обществ – 5, закрытых акционерных обществ – 1). Курирование деятельности этих организаций выполняется министром связи и информатизации или его заместителями (рис. 4). В состав организаций РУП «Белпочта», РУП «Белтелеком», РУП «БРТПЦ», ОАО «Белсвязьстрой», ОАО «Белремстройсвязь» входят филиалы, общее количество которых равно 30. Филиалы РУП «Белпочта» включают 90 узлов почтовой связи, филиалы РУП «Белтелеком» – 59 узлов электросвязи, в том числе 23 зональных и 23 районных узла. Наличие большого количества обособленных структурных

подразделений, их территориальная разобщенность и значительная протяженность линейно-кабельных сооружений существенно усложняют решение всех задач менеджмента и особенно защиты информации.



Рис. 4. Система курирования деятельности организаций, входящих в состав Министерства связи и информатизации Республики Беларусь

В отличие от продукции большинства промышленных предприятий, продукция организаций электросвязи является невещественной (т.е. она не может накапливаться на складах предприятия или дилерских центров), а процессы производства и потребления этой продукции неотделимы один от другого. Поэтому можно сделать вывод, что своевременность и качество предоставления услуг организациями электросвязи будет реализовано в случае обеспечения непрерывности их функционирования. При этом должны быть соблюдены следующие принципы [2]:

- доступность услуг электросвязи общего пользования;
- приоритет прав и законных интересов пользователей услуг электросвязи;
- равенство прав на получение услуг электросвязи;
- тайна телефонных и иных сообщений;
- устойчивость и управляемость сетей электросвязи;
- единство обязательных для соблюдения технических требований в области электросвязи.

Кроме этого, так как деятельность организаций электросвязи реализуется с применением критически важных объектов информатизации (КВОИ), то должно быть также обеспечено соблюдение требований Концепции национальной безопасности Республики Беларусь [4].

Исходя из вышеизложенного, можно сделать вывод о том, что аудит СМЗИ в организациях электросвязи Республики Беларусь должен проводиться в соответствии с принципом единоначалия, при котором один из руководителей органов государственного управления или представителей руководства организаций электросвязи утверждает графики и регламенты проведения аудита СМЗИ, а также осуществляет его итоговый контроль. В случае, если аудит является внеплановым, то целесообразной представляется также организация его промежуточного контроля со стороны названных субъектов.

Разработка критериев аудита системы защиты информации в организациях электросвязи

Любой аудит должен проводиться в соответствии с принципом критеральности (т.е. по согласованным критериям). К критериям проведения аудита СМЗИ в организациях электросвязи Республики Беларусь авторами предложено относить следующие:

- Конституцию Республики Беларусь;
- концепцию национальной безопасности Республики Беларусь;
- закон Республики Беларусь «Об информации, информатизации и защите информации»;

- закон Республики Беларусь «Об электросвязи»;
 - положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации;
 - Постановление Совета Министров Республики Беларусь от 30.03.2012 № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации»;
 - СТБ ISO/IEC 2701–СТБ ISO/IEC 27001-2011 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
 - политику защиты информации (при ее наличии);
 - внутренние документы организации (правила, процедуры, регламенты, требования), регулирующие деятельность, направленную на обеспечение защиты информации.
- В табл. 1 представлено описание предложенных критериев.

Таблица 1. Описание критериев проведения аудита системы защиты информации в организациях электросвязи

№ п/п	Наименование НТПА	Описание критерия
1	Постановление Совета Министров Республики Беларусь от 30.03.2012 № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации».	Проверка наличия в организации объектов, относящихся к КВОИ
2	Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации.	Проверка порядка отнесения объектов информатизации к КВОИ и обеспечение их безопасности (при наличии)
3	Политика защиты информации в организации	Проверка полноты мер, применяемых на организации для защиты КВОИ
4	Закон Республики Беларусь «Об электросвязи»	Проверка мер, применяемых для защиты тайны телефонных и иных сообщений (статья 54) и баз данных операторов электросвязи (статья 56)
5	Закон РБ «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455-3	Проверка мер, применяемых для защиты информации: правовых; организационных и технических (статья 29)
6	Концепция национальной безопасности Республики Беларусь (в части информационной безопасности)	Проверка мер, применяемых для защиты информации от внутренних и внешних угроз национальной безопасности в информационной сфере
7	Конституция Республики Беларусь	Проверка мер, применяемых для защиты субъектов 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 (статья 28)
8	Иные внутренние документы организации, регулирующие деятельность, направленную на обеспечение защиты информации	Проверка корректности применения основных терминов в области защиты информации (см. табл. 2)

В основе любой жизнедеятельности общества лежит соответствующий понятийный аппарат, определенный в нормативных и правовых актах государства. В связи с этим авторами статьи проанализированы определения основных терминов в сфере СМЗИ, используемые в основных руководящих документах (табл. 2).

Таблица 2. Основные термины в области защиты информации и документы, в которых регламентируется их использование

Наименование документа	Используемые термины	Свойства информации
Закон Республики Беларусь «Об информации, информатизации и защите информации»	Защита информации	конфиденциальность, целостность, доступность, подлинность, сохранность
СТБ ГОСТ Р 50922-2006 Защита информации Основные термины и определения	Защита информации; безопасность информации	конфиденциальность, целостность, доступность
СТБ ISO/IEC 27000-2012 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь.	Информационная безопасность	конфиденциальность, целостность, доступность (подлинность, подотчетность, неотказуемость, достоверность)

Из табл. 2 видно, что действующие в Республике Беларусь НТПА не дают однозначных определений терминов, используемых в области защиты информации, а в некоторых случаях вступают в противоречия между собой. Несмотря на существующие проблемы в вопросе терминологии, можно говорить об однозначности определений следующих основных регламентированных терминов.

1. Защита информации – комплекс правовых, организационных и технических мер направленных на обеспечение конфиденциальности, целостности, подлинности, доступности, сохранности и других свойств информации.

2. Безопасность информации (или информационная безопасность) – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность, доступность и другие свойства информации при ее обработке техническими средствами.

3. Система менеджмента защиты информации – обязательная составляющая системы менеджмента организации электросвязи, включающая в себя политики, процедуры, рекомендации и связанные с ними человеческие ресурсы, инфраструктуру и производственную среду, целью которых являются создание, внедрение, функционирование, мониторинг, анализ, поддержка и улучшение системы защиты информации организации.

Таким образом, аудиторы могут свидетельствовать о корректности внутренних документов аудируемой организации, регулирующих деятельность, направленную на обеспечение защиты информации, в случае, если употребляемые в тексте этих документов термины регламентированы представленными в табл. 2 документами.

Основные этапы аудита системы менеджмента защиты информации в организациях электросвязи

В [5] представлен перечень этапов, которые необходимо выполнять при проведении аудита СМЗИ в организациях. Суть каждого из этапов определяется спецификой деятельности аудируемой организации. В табл. 3 представлено описание предложенных подходов к реализации принципа поэтапности аудита СМЗИ в организациях электросвязи Республики Беларусь.

Таблица 3. Подходы к выполнению основных этапов аудита СМЗИ и результаты этих этапов

Номер этапа	Наименование этапа	Предложенный подход к выполнению этапа	Результаты этапа
1	Организация проведения аудита	Установление целей и задач проведения аудита в соответствии с его критериями. Определение временных рамок аудита	План проведения аудита
2	Подготовка к проведению аудита	Установление перечня КВОИ, используемых в аудируемой организации. Выбор с целью проверки внутренних документов организации. Определение основных угроз СМЗИ аудируемой организации	1. Список аудируемых отделов (сотрудники которых при выполнении своих должностных обязанностей используют КВОИ). 2. Список сопровождающих лиц, ответственных за обеспечение доступа аудитора к КВОИ организации. 3. Контрольные листы со списком анкетных вопросов для руководителей и сотрудников аудируемых отделов.
3	Проведение аудита	Опрос руководителей и сотрудников аудируемых отделов с использованием подготовленных контрольных листов. Наблюдение за работой аудируемых отделов. Проверка выбранных на этапе 2 документов.	Свидетельства аудита, в которых представлены данные о результатах проведенного опроса
4	Анализ данных, полученных в ходе проведения аудита	Проверка данных, представленных в свидетельствах, на соответствие критериям аудита	Перечень несоответствий
5	Подготовка отчета по результатам аудита	Структурирование в единый документ данных, полученных в ходе проведения аудита	Проект отчета о результатах проведения аудита
6	Завершение аудита	Проверка данных, представленных в проекте отчета о результатах проведения аудита, на соответствие плану аудита	Утверждение отчета о результатах проведения аудита у лица, ответственного за его итоговый контроль

Применение предложенных подходов будет способствовать структурированности аудита СМЗИ в организациях электросвязи Республики Беларусь.

Так как срок действия выдаваемых организациям Республики Беларусь сертификатов систем менеджмента качества составляет три года [6], то целесообразно проведение планового аудита СМЗИ в организациях электросвязи с периодичностью один раз в три года.

Заключение

Актуальность проведения аудита СМЗИ в организациях электросвязи Республики Беларусь обуславливается тем, что в настоящее время сфера услуг электросвязи является наиболее привлекательной для инвестирования. При этом большая часть инвестиций осуществляется за счет собственных средств государственных предприятий и бюджета.

В работе сформулированы и обоснованы следующие принципы аудита СМЗИ в организациях электросвязи Республики Беларусь:

1) единоначалие (один из руководителей органов государственного управления или представителей руководства организаций электросвязи утверждает графики и регламенты проведения аудита СМЗИ, а также осуществляет его итоговый контроль);

2) критериальность (основными критериями аудита СМЗИ организаций электросвязи следует считать ряд НТПА Республики Беларусь [2, 4, 7], а также внутренние документы аудируемой организации);

3) поэтапность (выполнение каждого из этапов аудита СМЗИ организаций электросвязи в соответствии с предложенными авторами статьи принципами).

Регулярность проведения аудита СМЗИ в организациях электросвязи будет способствовать повышению эффективности инвестиций, осуществляемых в сферу услуг электросвязи и уменьшению количества потенциальных внутренних угроз для экономической составляющей национальной безопасности Республики Беларусь.

METHOD'S REALIZATION PRINCIPLES OF INFORMATION PROTECTION MANAGEMENT SYSTEM AUDITING AT TELECOMMUNICATION COMPANIES

V.A. BOIPRAV, L.L. UTIN

Abstract

The evaluation of the activity specifics of Belarus telecommunication companies is made. The realization principles of information protection systems auditing method in these companies is grounded with use of the evaluation results and the requirements of Belarus normative and legal documents in the spheres of information security and telecommunication.

Keywords: audit, telecommunication company, system of information protection.

Список литературы

1. Информационное общество в Республике Беларусь. Статистический сборник / Под ред. И.В. Медведевой. Минск, 2015.
2. Закон Республики Беларусь от 19 июля 2005 г. № 45-З «Об электросвязи».
3. Указ Президента Республики Беларусь от 16 октября 2009 г. № 510 «О совершенствовании контрольной (надзорной) деятельности в Республике Беларусь».
4. Указ Президента Республики Беларусь от 09 ноября 2010 г. № 575 «Об утверждении концепции национальной безопасности».
5. ISO/IEC 27001:2013. Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
6. Технический институт сертификации и испытаний. [Электронный ресурс]. – Режим доступа: http://www.tisi.by/stb_smk_process.html. – Дата доступа: 07.07.2016.
7. Постановление Совета Министров Республики Беларусь от 30.03.2012 № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации».