УДК 004.056:654

МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ ОТРАСЛИ СВЯЗИ

В.А. БОЙПРАВ, О.В. БОЙПРАВ, Л.М. ЛЫНЬКОВ

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

Поступила в редакцию 10 апреля 2012

Проведен анализ мероприятий, подлежащих реализации непосредственно перед проведением процедуры составления или дополнения стратегической и тактической политик информационной безопасности предприятия отрасли связи, включающего в себя несколько филиалов и структурных подразделений.

Ключевые слова: аудит системы информационной безопасности, информационная безопасность, отрасль связи, стратегическая политика информационной безопасности, тактическая политика информационной безопасности.

Введение

Согласно Закону Республики Беларусь от 19 июля 2005 г. №45-З, измененному и дополненному 22 декабря 2011 г., деятельность в области электросвязи в Республике Беларусь должна осуществляться на основе принципов доступности услуг электросвязи общего пользования, приоритета прав и законных интересов пользователей услуг электросвязи, равенства прав на получение услуг электросвязи, тайны телефонных и иных сообщений, устойчивости и управляемости сетей электросвязи, единства обязательных для соблюдения технических требований в области электросвязи [1]. Реализация перечисленных принципов должна сопровождаться реализацией мероприятий по обеспечению информационной безопасности (ИБ) организации отрасли связи. Причем совокупность данных мероприятий следует своевременно отображать в политике информационной безопасности (ПИБ). Ее объем и структура определяются размером организации и количеством ее персонала.

В Республике Беларусь крупнейшей организацией в отрасли связи является республиканское унитарное предприятие (РУП) «Белтелеком», предоставляющее населению и организациям страны услуги телеграфа, телефонии, сети Интернет, проводного вещания, хостинга и цифрового интерактивного телевидения. На сегодняшний день количество абонентов РУП «Белтелеком» составляет более 4,5 миллионов физических и юридических лиц. При этом стратегическая цель РУП «Белтелеком» состоит в своевременности удовлетворения спроса на перечисленные услуги.

РУП «Белтелеком» включает в себя 10 филиалов: Брестский филиал, Витебский филиал, Гомельский филиал, Гродненский филиал, Могилевский филиал, Минский филиал, филиал «Минская городская телефонная сеть», филиал «Междугородная связь», филиал «Минская телеграфно-телефонная станция», филиал «Подсобное сельское хозяйство», а также 2 структурных подразделения в составе аппарата управления («Международный центр коммутации», «Информационно-расчетный центр»). Поэтому для РУП «Белтелеком», наряду с дополнением стратегической (общей) ПИБ, следует составлять и/или дополнять тактические (частные) ПИБ, описывающие совокупность мер, которые следует предпринимать для обеспечения ИБ филиалов и структурных подразделений. Перед дополнением стратегической ПИБ РУП «Белтелеком» и дополнением/составлением тактических ПИБ его филиалов (структурных подразделений), следует провести аудит его системы ИБ. На основании результатов аудита определяется

базовая система актуальных мер по обеспечению ИБ организации. Данные меры позволяют уменьшить риски ИБ до приемлемой величины.

Последовательность действий при проведении аудита системы информационной безопасности предприятия

С целью ускорения процедуры проведения аудита системы ИБ РУП «Белтелеком» следует назначить 12 аудиторских групп и закрепить за каждой из них определенный филиал (структурное подразделение).

На первом этапе аудита системы ИБ РУП «Белтелеком» руководителем аудиторских групп должно проводиться анкетирование генерального директора организации и директоров ее филиалов (структурных подразделений). Перечень основных вопросов для анкет представлен в таблице [2].

Перечень основных вопросов для анкетирования генерального директора организации и директоров ее филиалов (структурных подразделений)

Кому адресован вопрос	Формулировка вопроса
Генеральный директор организации	Проведена ли классификация информации, обрабатываемой в рамках информационной системы Вашей организации?
	Как давно обновлялась стратегическая ПИБ Вашей организации?
	Создан ли в РУП «Белтелеком» форум для обсуждения стратегической и тактической ПИБ и информационных рисков?
	Проводятся ли среди руководства РУП «Белтелеком» регулярные совещания по вопросам координации действий по поддержанию режима безопасности? Если да, то как часто?
	Проведено ли разграничение доступа к информационной системе Вашей организации?
Директора филиалов (структурных подразделений) организации	Ознакомлены ли Вы со стратегической ПИБ РУП «Белтелеком»?
	Есть ли у Вашего филиала (структурного подразделения) тактическая ПИБ?
	Если есть, то как давно она обновлялась?
	Есть ли в Вашем филиале (структурном подразделении) сотрудник, отвечающий за принятие мер по обеспечению ИБ и контроль выполнения стратегической и тактической (при ее наличии) ПИБ РУП «Белтелеком»?
	Проводите ли Вы с руководителями отделов своих филиалов (структурных подразделений) совещания по вопросам ИБ? Если да, то как часто?
	Проведена ли классификация информации, обрабатываемой в рамках информационной системы Вашего филиала (структурного подразделения)?
Генеральный директор и директора филиалов (структурных подразделений) организации	Доводите ли Вы до сведения нанимаемых сотрудников положения стратегической ПИБ РУП «Белтелеком» и тактических ПИБ его филиалов (структурных подразделений)?
	Когда в последний раз руководители отделов Вашей организации, работающих с информационной системой, проходили обучение по вопросам ИБ?
	Когда в последний раз в Вашей организации проводился аудит системы ИБ?
	Были ли ознакомлены руководители отделов Вашей организации, работающих с информационной системой, с результатами проведенного аудита?
	Проходила ли система защиты информационной системы Вашей организации аттестацию в соответствии с «Положением о порядке аттестации систем защиты информации» утвержденным Постановлением Совета Министров Республики Беларусь от 26.05.2009г. № 675? [3]

В рамках второго этапа экспертами аудиторских групп должна осуществляться проверка защищенности корпоративной сети каждого из филиалов: установление частоты обновления антивирусного программного обеспечения и наличия (выполнения) разделов ПИБ, касающихся политики управления компьютерными паролями и разграничения доступа к данным персональных компьютеров. В рамках второго этапа следует провести анкетирование с системными администраторами корпоративной сети организации, а также корпоративных сетей ее филиалов (структурных подразделений). Среди основных вопросов для анкет системных администраторов должны быть следующие. Установлено ли на персональных компьютерах сотрудников Вашего филиала (структурного подразделения) антивирусное программное обеспечение? Проверка жестких и съемных дисков персональных компьютеров сотрудников Вашего филиала на наличие вирусов производится вручную, либо с использованием сканеров? Произведена ли настройка источника и периодичности обновления вирусных сигнатур антивирусного программного обеспечения? Знают ли сотрудники Вашего филиала последовательность действий при обнаружении вируса антивирусным программным обеспечением? [4]

На третьем этапе следует проводить проверку наличия и исправности систем контроля и управления доступом (дверей, замков, оконных решеток и т.д.), систем охранной и противопожарной сигнализации в помещениях, где располагается оборудование, диагностику их климатических условий (температура и влажность воздуха, наличие вентиляционной системы и системы кондиционирования) [5].

Результаты аудита ИБ филиалов должны быть сведены в итоговые отчеты ответственными по каждой из аудиторских групп. Директора филиалов (структурных подразделений) должны быть ознакомлены с положениями этих отчетов перед проведением собрания по закрытию аудита.

На основании данных итоговых отчетов руководитель аудиторских групп готовит общий итоговый отчет и доносит его положения на собрании по закрытию аудита до генерального директора организации и директоров ее филиалов (структурных подразделений).

Обработка результатов аудита системы информационной безопасности предприятия

На основании положений общего итогового отчета об аудите системы ИБ РУП «Белтелеком» осуществляется дополнение его стратегической ПИБ. В состав рабочей группы по дополнению стратегической ПИБ РУП «Белтелеком» следует включать генерального директора организации, заместителя генерального директора по техническим вопросам, заместителя генерального директора по персоналу, директоров филиалов (структурных подразделений), начальника службы безопасности, начальника юридического отдела, технического писателя, а также независимого эксперта по разработке ПИБ (руководителя аудиторских групп, проводивших аудит ИБ организации).

На основании положений итоговых отчетов об аудите системы ИБ филиалов (структурных подразделений) РУП «Белтелеком», а также положений дополненной стратегической ПИБ осуществляется дополнение его тактических ПИБ. В состав рабочей группы по дополнению тактических ПИБ РУП «Белтелеком» следует включать директоров филиалов (структурных подразделений), главных инженеров, начальника службы безопасности, юристов, технических писателей, а также независимых экспертов по разработке ПИБ (ответственных по аудиторским группам, проводившим аудит ИБ филиалов (структурных подразделений)).

Положения стратегической и тактической ПИБ РУП «Белтелеком» для его сотрудников должны носить не рекомендательный, а обязательный характер. Ответственность за нарушение положений ПИБ должна быть четко определена и возложена на директоров филиалов (структурных подразделений) РУП «Белтелеком».

Во всех филиалах (структурных подразделениях) должен быть назначен сотрудник, отвечающий за принятие мер по обеспечению ИБ и контроль выполнения положений стратегической и тактической ПИБ (в случае, если он не был назначен ранее). Кроме того, необходимо назначить сотрудника, который будет вести контроль выполнения всеми филиалами (структурными подразделениями) РУП «Белтелеком» положений стратегической ПИБ путем регулярного проведения проверок.

За нарушение положений ПИБ должны быть предусмотрены конкретные дисциплинарные, административные взыскания и материальная ответственность, возлагаемые как на работника, не соблюдающего положения ПИБ, так и на сотрудника филиала (структурного подразделения), осуществляющего контроль выполнения ПИБ, а также директора данного филиала (структурного подразделения).

С изменениями и дополнениями стратегической и тактической ПИБ РУП «Белтелеком», а также с перечнем мер, предпринимаемых в случае невыполнения ее положений, должен быть под роспись ознакомлен каждый сотрудник организации, имеющий доступ к информационной системе.

При этом при внесении новых положений в ПИБ стоит учитывать то, что они должны однозначно истолковываться сотрудниками, для которых предназначены. Кроме того, соблюдение положений ПИБ не должно в значительной степени оказывать влияния на темпы выполнения сотрудниками своих прямых обязанностей, прописанных в должностных инструкциях.

В организации должны быть предусмотрены меры по реагированию на нарушение положений ПИБ, в частности – оповещение об инциденте сотрудников организации, процедуры восстановления утерянных либо поврежденных данных, механизмы сбора доказательств нарушения положений стратегической либо тактической ПИБ, проведение расследования, выявление нарушителей и привлечение нарушителей к ответственности.

Заключение

Регулярно проводимый аудит системы безопасности каждого из филиалов (структурных подразделений) РУП «Белтелеком» позволит поддерживать актуальность положений его стратегической и тактической ПИБ, а также более рационально управлять денежными средствами, направляя их не на восстановление работоспособности телекоммуникационного оборудования и целостности данных, обрабатываемых в рамках информационной системы, а на расширение пакетов и улучшение качества услуг, предоставляемых населению и организациям страны, модернизацию телекоммуникационного оборудования, повышение профессиональной грамотности сотрудников.

METHODS FOR MAINTENANCE INFORMATION SECURITY IN THE TELECOMMUNICATION SECTOR ORGANIZATION

V.A. BOIPRAV, O.V. BOIPRAV, L.M. LYNKOU

Abstract

The analysis of measures to be implemented before the procedure of preparation or add strategic and tactical information security policies enterprise communications industry, including a number of subsidiaries and business units, is conducted.

Литература

1. Закон Республики Беларусь от 19 июля 2005 г. №45-З «Об электросвязи».
2. ISO 27001-2005. Системы управления информационной безопасностью.
3. Система защиты информации. [Электронный ресурс]. Режим доступа: http://itsec.by/audit-informatsionnoy-bezopasnosti-primer/.
4. Аудит информационной безопасности. [Электронный ресурс]. Режим доступа: http://itsec.by/predvaritelnaya-obshhaya-ocenka-sistemy-zashhity-informacii-gosudarstvennoj-informacionnoj-sistemy-anketa-voprosnik-chast-2/.
5. *Бойправ В.А., Бойправ О.В., Лыньков Л.М.* // Матер. XVII Межд. науч.-техн. конф. «Современные средства связи». Минск, 2012. С. 249.