# ОСОБЕННОСТИ ПОДГОТОВИТЕЛЬНОГО ЭТАПА АУДИТА СИСТЕМЫ МЕНЕДЖМЕНТА ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИЯХ ЭЛЕКТРОСВЯЗИ

В.А. БОЙПРАВ, Л.Л. УТИН

*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

*Поступила в редакцию 11 декабря 2017*

**Аннотация.** Проанализированы особенности подготовительного этапа аудита системы менеджмента защиты информации организаций электросвязи, выявлены противоречия и рассмотрены пути их решения. Предложено в ходе его реализации категорировать организации электросвязи в зависимости от специфики их деятельности и количества классов критически важных объектов информатизации, доступ к которым имеют сотрудники этих организаций. На основе результатов категорирования возможно сформировать индивидуальный перечень ТНПА и вопросов для анкетирования сотрудников организаций электросвязи.

*Ключевые слова:* аудит, защита информации, организации электросвязи.

**Abstract.** The features of preparatory phase of telecommunication organizations information security management system's audit are analyzed. It is proposed to classify the telecommunication organizations depending on the specific them activities and the number of critically important informatization object classes, which have access to the staff of these organizations. It's possible to generate a ROV list and questions for telecommunications companies employees survey.

*Keywords:* audit, information security, telecommunication organization.

**Doklady BGUIR. 2018, Vol. 111, No. 1, pp. 43-50**
**Preparatory stage features of information security management system audit in telecommunication organizations**
**V.A. Boiprav, L.L. Utin**

## Введение

Деятельность организаций электросвязи сопряжена с созданием, эксплуатацией и обслуживанием критически важных объектов информатизации (КВОИ), нарушение функционирования которых может привести к негативным последствиям в информационной и экономической сферах национальной безопасности [1]. В связи с этим одними из составляющих системы менеджмента защиты информации организаций электросвязи являются процедуры по внутреннему и внешнему контролю их КВОИ, регламентированному соответственно Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» и приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2012 г. № 42 «Об утверждении Инструкции о порядке проведения внешнего контроля за обеспечением безопасности критически важных объектов информатизации» [1, 2]. В работе [3] показано, что аудит системы менеджмента защиты информации в организациях электросвязи должен выполняться в соответствии с принципом поэтапности. Важным этапом в этом процессе является подготовительный, так как в ходе него определяются и классифицируются КВОИ, используемые аудируемой организацией, реализуемые по отношению к ним угрозы безопасности, а также разрабатываются контрольные листы с вопросами для сотрудников, которые имеют доступ к указанным объектам. Цель настоящей работы заключается в установлении особенностей реализации подготовительного этапа в ходе проведения аудита системы менеджмента защиты информации организаций электросвязи в зависимости от используемых ими классов КВОИ. Для достижения поставленной цели необходимо решить следующие задачи:

1) установить классы используемых организациями электросвязи КВОИ в зависимости от специфики деятельности этих организаций;

2) определить уязвимости КВОИ, используемых организациями электросвязи, в зависимости от специфики их деятельности и класса указанных объектов и классифицировать потенциальные угрозы безопасности этих объектов (количество угроз, воздействующих на уязвимость, определяет риск информационной безопасности);

3) сформировать перечень ТНПА, которые могут быть использованы в целях составления вопросов для анкетирования сотрудников аудируемых организаций электросвязи на основе результатов решения первых двух задач.

Решение по очередности каждой из указанных задач позволит сократить временные и материальные затраты на проведение аудита и соответствует реализации процедур подготовительного этапа аудита системы менеджмента защиты информации в организациях электросвязи.

## Классификация организаций электросвязи

В зависимости от специфики деятельности организации электросвязи могут быть разделены на следующие категории:

1 – организации, занимающиеся строительством сетей и сооружений электросвязи;

2 – организации, занимающиеся предоставлением услуг электросвязи;

3 – организации, занимающиеся проектированием сетей и сооружений электросвязи;

4 – организации, являющиеся органами, осуществляющими государственное регулирование и управление в области электросвязи.

Порядок ранжирования рассматриваемых организаций по категориям определен исходя из того, к какому количеству классов КВОИ имеют доступ сотрудники этих организаций (рис. 1).


Рис. 1. Перечень активов КВОИ, используемых сотрудниками организации электросвязи

Основные особенности использования активов КВОИ сотрудникам различных организаций представлены в табл. 1.

Таблица 1. **Особенности использования КВОИ и их активов сотрудниками организаций различных категорий**

| Категория организации | Наименование активов КВОИ, используемых сотрудниками организации [4] | Особенности использования активов КВОИ сотрудниками организации | Классы используемых КВОИ [5] |
|---|---|---|---|
| 1 | Аппаратно-программные ресурсы (средства и линии электросвязи) | Строительство и пуско-наладка | А1, А2, Б1, Б2, Б3, В3 |
| 2 | Информация (базы данных) | Хранение и обработка персональных данных абонентов | А2, Б2, Б3, В3 |

| | | | |
|---|---|---|---|
| | Аппаратно-программные ресурсы (средства электросвязи) | Обслуживание и эксплуатация | |
| 3 | Информация (документы и базы данных) | Создание, хранение и обработка данных, касающихся архитектуры сетей электросвязи, включая сведения об аппаратно-программных средствах, используемых в таких сетях | А1, А2, А3,Б2 |
| 4 | Информация (документы и базы данных) | Создание, хранение и обработка данных об организационно-техническом обеспечении функционирования сетей электросвязи, использовании радиочастотного спектра, а также о мероприятиях по защите сетей электросвязи от несанкционированного доступа к ним и передаваемым сообщениям | А1, А2, А3 |

Кроме того, авторами установлено, что количество организаций, отнесенных к категории 1, значительно превышает количество организаций, отнесенных к категориям 2–4 (табл. 2) [6–8].

Таблица 2. **Количество организаций электросвязи различных категорий**

| Категория организации | Количество организаций указанной категории |
|---|---|
| 1 | 1765 |
| 2 | 380 |
| 3 | 47 |
| 4 | 4 |

Наиболее сложная ситуация сложилась на рынке услуг по строительству сетей, систем и сооружений электросвязи. После отмены лицензий на осуществление этого вида деятельности количество организаций, занимающихся строительством сетей и сооружений электросвязи, начало расти. Значительная часть этих организаций осуществляла строительство промышленных и жилых объектов, но сокращение финансирования этого сектора экономики вынуждает их изменять направление своей деятельности. Возросшая конкуренция на рынке строительства объектов электросвязи способствовала снижению стоимости выполняемых работ при одновременном повышении уязвимости КВОИ и всех сетей электросвязи в целом. Принцип отбора подрядных организаций на выполнение работ по строительству объектов электросвязи не включает требований по наличию собственной системы менеджмента защиты информации и не предусматривает проведение проверки эффективности ее функционирования. Мелкие и средние строительные компании постоянно прибегают к практике приема на работу специалистов, набранных по рекламным объявлениям, для реализации конкретных объектов. Настоящая практика приводит к бесконтрольному допуску большого количества случайных людей на КВОИ и дает возможность вмешаться в процесс их функционирования или вывести из эксплуатации. Стремительный рост количества подрядных организаций при отсутствии какого-нибудь регулирования их деятельности на сетях электросвязи требует отнести их к 1 категории организаций с точки зрения количества уязвимостей КВОИ.

Увеличение организаций, получивших лицензии на предоставление услуг электросвязи, (рис. 2) и имеющаяся у большинства из них возможность подключиться к телефонным сетям общего пользования создают угрозу нарушения работоспособности КВОИ. Количество этих организаций и количество используемых классов КВОИ позволяет отнести их ко 2 категории организаций с точки количества уязвимостей КВОИ.

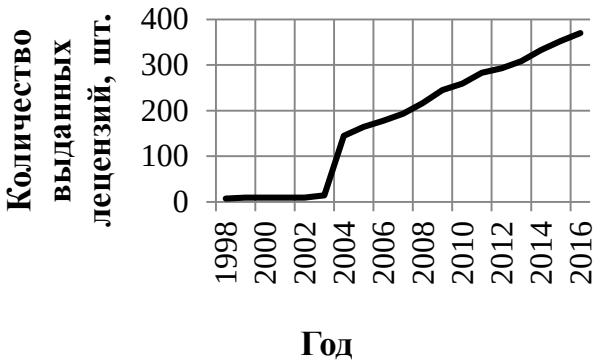


Рис. 2. Динамика изменения количества организаций,
получивших лицензию на предоставление услуг электросвязи

Организации, занимающиеся проектированием сетей, систем и сооружений связи можно отнести к 3 категории организаций с точки зрения количества КВОИ, доступ к которым имеют их сотрудники, по причине ограниченности прямого доступа на КВОИ и сетям электросвязи. Органы государственного управления, занимающиеся регулированием в области электросвязи, отнесены к 4 категории из-за высокой квалификации персонала и наличия в их структуре специалистов по спецработе.

## Классификация потенциальных угроз безопасности КВОИ, используемых организациями электросвязи различных категорий

В [4] показано, что для описания моделей угроз безопасности КВОИ необходимо использовать следующие понятия: источник угрозы; актив КВОИ, на который направлена угроза; уязвимость, обуславливающая реализацию угрозы. Источниками рассматриваемых угроз в соответствии с [4] являются лица, относящиеся или не относящиеся к числу сотрудников организации (так называемые внутренние или внешние нарушители соответственно). Угроза является следствием преднамеренных или непреднамеренных действий таких лиц на уязвимость. Установлено, что причинами возникновения этой уязвимости, обуславливающей реализацию угрозы безопасности КВОИ, могут быть следующие:

– уязвимости, характерные для актива КВОИ;

– уязвимости, характерные для комплекса средств безопасности КВОИ;

– преднамеренное или непреднамеренное невыполнение сотрудниками организации положений ее политики информационной безопасности.

Результатом реализации угроз безопасности КВОИ классов Б3, В3 является нарушение свойств целостности (подлинности, сохранности) и доступности информации, обрабатываемой этими объектами, а угроз безопасности КВОИ классов А1, А2, Б1, Б2 – нарушение двух указанных свойств, а также свойства конфиденциальности информации, обрабатываемой этими объектами. Источниками угроз могут быть также неблагоприятные погодные условия и природные катаклизмы. Результат реализации угроз, исходящих от таких источников, – нарушение свойств целостности и доступности информации, обрабатываемой КВОИ, независимо от того, к какому классу относится этот объект. Наименования активов КВОИ, на которые направлены угрозы безопасности, представлены в столбце 2 табл. 1.

В табл. 3 представлен установленный авторами перечень основных причин возникновения уязвимостей, обуславливающих реализацию угроз безопасности КВОИ, к которым имеют доступ сотрудники организаций электросвязи, в зависимости от категории последних.

Таблица 3. **Перечень потенциальных уязвимостей КВОИ организаций электросвязи**

| Категория организации | Категория информации, обрабатываемой КВОИ, по отношению к безопасности которого реализуется угроза [9] | Основные причины возникновения уязвимости, обуславливающей реализацию угрозы безопасности КВОИ |
|---|---|---|
| 1 | Государственные секреты, персональные данные, | 1. Побочные электромагнитные излучения средств и линий электросвязи. |

| | | |
|---|---|---|
| | служебная и коммерческая тайны | 2. Выход из строя средств и/или линий электросвязи ввиду их производственных дефектов (в том числе дефектов, обуславливающих их незащищенность от внешних факторов). |
| 1 | Государственные секреты, персональные данные, служебная и коммерческая тайны | 3. Нарушение работоспособности или ошибки в проектировании систем охранной и пожарной сигнализации, относящихся к комплексу средств безопасности КВОИ.<br>4. Полное или частичное несоблюдение требований к технической укрепленности КВОИ или их отдельных конструктивных элементов [10] (линий электросвязи, используемых для соединения КВОИ, расположенных в пределах разных контролируемых зон).<br>5. Некорректные подключение и настройка средств электросвязи.<br>6. Нарушение контрольно-пропускного режима на КВОИ.<br>7. Нарушение порядка перемещения лиц, не относящихся к числу сотрудников организации, в пределах контролируемой зоны КВОИ.<br>8. Преднамеренное или непреднамеренное повреждение средств и линий электросвязи лицами из числа внутренних или внешних нарушителей.<br>9. Замедление процесса реализации мероприятий по устранению повреждений средств и линий электросвязи.<br>10. Разглашение сотрудниками организации сведений о местах расположения и технических характеристиках средств, линий и сооружений электросвязи как активов КВОИ, о заказчиках и ходе работ по строительству линий и сооружений электросвязи и пуско-наладке средств электросвязи. |
| 2 | Персональные данные, служебная и коммерческая тайны | 1. Причины, описанные в п. 2–4, 6–9 строки 3 настоящей таблицы.<br>2. Преднамеренное или непреднамеренное разглашение сотрудниками организации третьим лицам данных об абонентах из числа как физических, так и юридических лиц.<br>3. Преднамеренное или непреднамеренное разглашение сотрудниками организации третьим лицам данных об используемых в организации системах тарификации услуг электросвязи. |
| 3, 4 | Государственные секреты, служебная тайна | 1. Побочные электромагнитные излучения средств вычислительной техники, используемых для создания, обработки и хранения электронных документов и баз данных, в которых содержится информация ограниченного распространения.<br>2. Невыполнение разграничения доступа к электронным документам и базам данных, в которых содержится информация ограниченного распространения.<br>3. Невыполнение шифрования электронных документов и баз данных, в которых содержится информация ограниченного распространения.<br>4. Несвоевременное обновление программных средств, относящихся к комплексу средств безопасности КВОИ.<br>5. Отсутствие или неиспользование выделенных помещений для проведения переговоров. |

На основе предложенного категорирования организаций электросвязи и классификации потенциальных угроз безопасности используемых ими КВОИ можно рекомендовать использование следующего перечня ТНПА в целях составления вопросов для анкетирования сотрудников этих организаций (таблица 3):

1. Конституция Республики Беларусь.

2. Закон Республики Беларусь «Об электросвязи».

3. Концепция национальной безопасности Республики Беларусь (в части информационной безопасности).

4. Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации.

5. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь 16.01.2015 № 3).

6. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30.04.2012 № 42.

7. ТКП 45-1.02-25-201-2014 Строительство Проектная документация Состав и содержание.

8. СТБ ISO/IEC 27001-2016 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

9. СТБ ISO/IEC 27000-2012 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь.

10. Политика защиты информации в организации.

11. Иные внутренние документы организации, регулирующие деятельность, направленную на обеспечение защиты информации.

Таблица 3. **Перечень ТНПА для составления вопросов для анкетирования сотрудников организаций электросвязи различных категорий**

| Категория организации электросвязи | Номер ТНПА из приведенного перечня |
|---|---|
| 1 | 1–11 |
| 2 | 1–6, 8–11 |
| 3 | 3–5, 7–11 |
| 4 | 1–4, 8–11 |

## Заключение

Предложен порядок реализации подготовительного этапа аудита системы менеджмента защиты информации организаций электросвязи, включающий в себя следующие процедуры:

1) установление классов КВОИ и классов активов КВОИ, к которым могут получать доступ сотрудники аудируемой организации электросвязи;

2) составление моделей потенциальных угроз безопасности КВОИ, используемых организациями электросвязи;

3) разработка перечня анкетных вопросов для сотрудников аудируемых организаций электросвязи на основе результатов, полученных в ходе реализации указанных процедур.

Предложено ранжировать перечень организаций электросвязи по четырем категориям в зависимости от специфики их деятельности: строительство, предоставление услуг электросвязи, проектирование сетей электросвязи, управление и регулирование деятельности организаций электросвязи. Показано, что количество классов КВОИ, к которым могут получать доступ сотрудники организаций электросвязи, зависит от специфики деятельности последних. Установлено, что сотрудники организаций, занимающихся строительством сетей и сооружений электросвязи (организаций категории 1), в процессе выполнения своих трудовых обязанностей имеют право получать доступ к КВОИ всех шести классов, определенных в СТБ 34.101.30-2007 (А1, А2, Б1, Б2, Б3, В3). В связи с этим в ходе аудита системы менеджмента защиты информации для сотрудников организаций категории 1 необходимо разрабатывать наибольшее количество анкетных вопросов, чем в ходе реализации аналогичных мероприятий по отношению к организациям категорий 2–4, специфика деятельности которых заключается соответственно в предоставлении услуг электросвязи, проектировании сетей электросвязи, управлении и регулировании деятельности организаций электросвязи.

## Список литературы


1. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации : Указ Президента Респ. Беларусь, 25 окт. 2011 г., № 486 // Нац. реестр правовых актов Респ. Беларусь. 2011. № 121. 1/13026.
2. Об утверждении Инструкции о порядке проведения внешнего контроля за обеспечением безопасности критически важных объектов информатизации : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 30 апр. 2012 г., № 42 // Нац. реестр правовых актов Респ. Беларусь. 2012. № 52. 7/2003.
3. Бойправ, В.А., Утин Л.Л. Принципы реализации методики аудита системы менеджмента защиты информации в организациях электросвязи // Докл. БГУИР. 2016. № 6 (100). С. 94–99.
4. ТКП 483-2013 (01019). Информационные технологии и безопасность. Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования. Минск : ОАЦ, 2013. 6 с.
5. СТБ 34.101.30-2007. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация. Минск : Белорус. гос. ин-т стандартизации и сертификации, 2007. 4 с.

6. Белорусский бизнес [Электронный ресурс]. – URL: http://www.bizby.ru (дата обращения: 01.11.2017).
7. Информационно-справочный портал [Электронный ресурс]. – URL: http://www.belarusinfo.by (дата обращения: 01.11.2017).
8. Список операторов, которым выданы лицензии на деятельность в области связи [Электронный ресурс]. – URL: http://www.mpt.gov.by/ru/licenzirovanie/spisok-operatorov-kotorym-vydany-licenzii-na-deyatelnost-v-oblasti-svyazi/ (дата обращения: 25.11.2017).
9. Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З // Нац. реестр правовых актов Респ. Беларусь. 2008. № 279. 12/1552.
10. Рабочий проект ТКП МВД Респ. Беларусь. Техническая укрепленность объектов. Правила проектирования. Минск : М-во внутренних дел Респ. Беларусь, 2014. 68 с.

## References

1. O nekotoryh merah po obespecheniju bezopasnosti kriticheski vazhnyh ob#ektov informatizacii : Ukaz Prezidenta Resp. Belarus', 25 okt. 2011 g., № 486 // Nac. reestr pravovyh aktov Resp. Belarus'. 2011. № 121. 1/13026. (in Russ.)
2. Ob utverzhdenii Instrukcii o porjadke provedenija vneshnego kontrolja za obespecheniem bezopasnosti kriticheski vazhnyh ob'ektov informatizacii : prikaz Operativno-analiticheskogo centra pri Prezidente Resp. Belarus', 30 apr. 2012 g., № 42 // Nac. reestr pravovyh aktov Resp. Belarus'. 2012. № 52. 7/2003. (in Russ.)
3. Bojprav, V.A., Utin L.L. Principy realizacii metodiki audita sistemy menedzhmenta zashhity informacii v organizacijah jelektrosvjazi // Dokl. BGUIR. 2016. № 6 (100). S. 94–99. (in Russ.)
4. TKP 483-2013 (01019). Informacionnye tehnologii i bezopasnost'. Bezopasnaja jekspluatacija i nadezhnoe funkcionirovanie kriticheski vazhnyh ob'ektov informatizacii. Obshhie trebovanija. Minsk : OAC, 2013. 6 s. (in Russ.)
5. STB 34.101.30-2007. Informacionnye tehnologii. Metody i sredstva bezopasnosti. Ob'ekty informatizacii. Klassifikacija. Minsk : Belorus. gos. in-t standartizacii i sertifikacii, 2007. 4 s. (in Russ.)
6. Belorusskij biznes [Electronic resource]. – URL: http://www.bizby.ru (access date: 01.11.2017). (in Russ.)
7. Informacionno-spravochnyj portal [Electronic resource]. – URL: http://www.belarusinfo.by (access date: 01.11.2017). (in Russ.)
8. Spisok operatorov, kotorym vydany licenzii na dejatel'nost' v oblasti svjazi [Electronic resource]. – URL: http://www.mpt.gov.by/ru/licenzirovanie/spisok-operatorov-kotorym-vydany-licenzii-na-deyatelnost-v-oblasti-svyazi/ (access date: 25.11.2017). (in Russ.)
9. Ob informacii, informatizacii i zashhite informacii : Zakon Resp. Belarus' ot 10 nojab. 2008 g. № 455-Z // Nac. reestr pravovyh aktov Resp. Belarus'. 2008. № 279. 12/1552. (in Russ.)
10. Rabochij proekt TKP MVD Resp. Belarus'. Tehnicheskaja ukreplennost' ob'ektov. Pravila proektirovanija. Minsk : M-vo vnutrennih del Resp. Belarus', 2014. 68 s. (in Russ.)

**Сведения об авторах**

Бойправ В.А., аспирант кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Утин Л.Л., к.т.н., доцент, начальник кафедры связи Белорусского государственного университета информатики и радиоэлектроники.

**Information about the authors**

Boiprav V.A., PG student of the information security department of Belarusian state university of informatics and radioelectronics.

Utin L.L., PhD, associate professor, head of telecommunication department of Belarusian state university of informatics and radioelectronics.

**Адрес для корреспонденции**

220013, Республика Беларусь,
Минск, ул. П. Бровки, 6,
Белорусский государственный
университет информатики и радиоэлектроники
тел. +375-33-602-78-88;
e-mail: name_abs@rambler.ru
Бойправ Владимир Андреевич

**Address for correspondence**

220013, Republic of Belarus,
Minsk, P. Brovka st., 6,
Belarusian state university
of informatics and radioelectronics
tel. +375-33-602-78-88;
e-mail: name_abs@rambler.ru
Boiprav Vladimir Andreevich