Электронный научный журнал «Век качества» ISSN 2500-1841 http://www.agequal.ru

2020, №2 http://www.agequal.ru/pdf/2020/AGE_QUALITY_2_2020.pdf

Ссылка для цитирования этой статьи:

Вайнзоф Л.А. Нормативное обеспечение средств противодействия угрозам сети связи общего пользования – фактор влияния на менеджмент качества услуг электросвязи // Электронный научный журнал «Век качества». 2020. №2. С. 59-83. Режим доступа: http://www.agequal.ru/pdf/2020/220005.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004.056; 654.1

Нормативное обеспечение средств противодействия угрозам сети связи общего пользования – фактор влияния на менеджмент качества услуг электросвязи

Вайнзоф Леонид Абрамович,

кандидат технических наук,

специалист Центра сертификации систем качества «Интерэкомс»

Нормативное обеспечение средств противодействия угрозам сети связи общего пользования (ССОП) – это широко развитая система документов разных уровней. Неизбежный прогресс в развитии глобальной сети электросвязи, усложнение средств и услуг электросвязи, появление новых или более строгих требований к содержанию и качеству этих услуг со стороны надзирающих органов и потребителей – всё это влечёт необходимость совершенствования существующей нормативной документации и создания новых документов.

Организации и предприятия, связанные с созданием и эксплуатацией сетей электросвязи или причастные к обеспечению безопасности функционирования этих сетей, должны постоянно осуществлять мониторинг и анализ соответствующей нормативной документации для своевременного выполнения её требований в своей деятельности.

В статье анализируется федеральное законодательство, устанавливающее основы деятельности в области связи на территории Российской Федерации, а также надотраслевые, межотраслевые и отраслевые стандарты, касающиеся услуг электросвязи в части защиты от информационных угроз.

Ключевые слова: сеть электросвязи, услуги электросвязи, сети связи общего пользования, безопасность функционирования сетей электросвязи, противодействие угрозам сети связи общего пользования, нормативное обеспечение, нормативная документация, стандарты, менеджмент качества.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Сеть электросвязи – одна из сложнейших технических систем, существующих в настоящее время. Она охватывает практически все необходимые человечеству районы планеты и обеспечивает миллиардам пользователей возможность обмена информацией. Существенной частью этой системы является Единая сеть электросвязи Российской Федерации, в состав которой, согласно Федеральному Закону от 07.07.2003 г. № 126-ФЗ «О связи» (редакция, действующая с 1.11 2019 г.)[1], входит сеть связи общего пользования (ССОП). В соответствии со ст. 13 этого Закона, ССОП «*предназначена для возмездного оказания услуг электросвязи любому пользователю услугами связи на территории Российской Федерации*». Поэтому качество услуг, оказываемых операторами сетей, входящих в состав ССОП, затрагивает интересы государства и подавляющего числа физических и юридических лиц, и её состояние является объектом пристального внимания со стороны управляющих и надзорных организаций.

Качество услуг электросвязи, а, следовательно, и требования к менеджменту этого качества зависят от множества факторов. Одним из важнейших внешних факторов является пакет соответствующих нормативных документов. Нормативное обеспечение устанавливает правила, определяющие всевозможные стороны жизни сети электросвязи: требуемые свойства и порядок работы её как единого целого, свойства и работу множества по разным критериям выделенных подсистем, взаимодействие этих подсистем и другие проблемы, вплоть до значений определённых параметров.

Нормативные документы могут быть разного уровня: от международных (они чаще всего излагаются как рекомендации, неисполнение которых, однако, реально исключено) и государственных (законы, постановления правительства и т.п.) до должностных инструкций на конкретных

[1] О связи: Федеральный Закон от 07.07.2003 № 126-ФЗ (ред., действующая с 1 ноября 2019 г.). - Режим доступа: http://www.pravo.gov.ru.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

предприятиях. Системы менеджмента качества организаций, оказывающих услуги электросвязи и причастных к такой деятельности, должны строиться с учётом требований этих документов.

Концепция информационной безопасности Сетей связи общего пользования Взаимоувязанной сети связи РФ

Исторически требования к качеству услуг электросвязи развивались в соответствии с ростом сетей, усложнением возможностей оборудования и потребностей пользователей, изменениями условий предоставления этих услуг.

Одна из серьёзных задач, связанных с поддержанием в рабочем состоянии и эксплуатацией сетей электросвязи, входящих в состав ССОП, касается рисков нарушения их целостности, устойчивости функционирования и безопасности. С учётом таких рисков Министерством Российской Федерации по связи и информатизации в 2002 г. была разработана Концепция информационной безопасности Сетей связи общего пользования Взаимоувязанной сети связи Российской Федерации[2]. В этом документе указано, что «*процесс глобализации информационно-телекоммуникационных комплексов, внедрение на ССОП России телекоммуникационных технологий, реализуемых преимущественно на аппаратно-программных средствах зарубежного производства, существенно обострили проблему зависимости качества процессов транспортирования информации от возможных преднамеренных и непреднамеренных воздействий нарушителя на передаваемые данные пользователя, информацию управления и аппаратно-программные средства, обеспечивающие эти процессы*». По мнению авторов Концепции, отсутствие в ССОП необходимых средств защиты делало её уязвимой по отношению к

[2] Концепция информационной безопасности Сетей связи общего пользования Взаимоувязанной сети связи РФ. - М., 2002.

возможным противоправным действиям. В связи с этим были поставлены задачи создания мер защиты ССОП и системы управления ею от возможностей несанкционированного доступа к предоставляемым услугам связи, преднамеренных воздействий нарушителя, активизации нарушителем вредоносных программ и других угроз. Концепция послужила основой для разработки в дальнейшем комплекса организационных и технических мер по обеспечению информационной безопасности ССОП, а также нормативных и методических документов, обеспечивающих ее реализацию. Система нормативных документов по безопасности ССОП в настоящее время внедрена и эффективно применяется. Благодаря углублению знаний о возможных угрозах и, как следствие, развитию и уточнению требований к защите от них, а также появлению новых технических возможностей соответствующее нормативное обеспечение продолжает развиваться.

Документы высшего уровня

Нормативным документом высшего уровня, устанавливающим основы деятельности в области связи на территории Российской Федерации, является Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (настоящая редакция действует с 01 ноября 2019 г.)[3]. Законом выделены следующие категории сетей, входящих в состав Единой сети электросвязи Российской Федерации:

- сеть связи общего пользования;
- выделенные сети связи;
- технологические сети связи, присоединенные к сети связи общего пользования;
- сети связи специального назначения и другие сети связи для передачи информации при помощи электромагнитных систем.

Законом установлено, что сеть связи общего пользования представляет

[3] О связи: Федеральный закон от 07.07.2003 г. № 126-ФЗ (ред. от 07.04.2020). - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_43224/.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

собой комплекс взаимодействующих сетей электросвязи. Входящие в состав ССОП сети могут определяться обслуживаемой территорией и номерным ресурсом, либо технологией реализации оказания услуг связи. При необходимости и наличии технической и номерной возможностей часть технологической сети связи может быть присоединена к сети связи общего пользования с переводом в категорию сети связи общего пользования. ССОП имеет присоединение к сетям связи общего пользования иностранных государств.

Закон «О связи» регламентирует правила оказания услуг связи, включая, в частности, обязанности операторов связи, оплату услуг связи и предусмотренные льготы. Отдельной статьей выделены особенности оказания услуг для нужд органов государственной власти, обороны страны, безопасности государства и обеспечения правопорядка.

Законом учтено наличие рисков, сопровождающих строительство и эксплуатацию сетей связи. В соответствии с этим в требованиях к деятельности в области связи ст. 7 определена защита сетей связи и сооружений связи. Кроме того, Федеральным законом от 01.05.2019 № 90-ФЗ [4] в Закон «О связи» включена глава, определяющая требования к обеспечению устойчивого, безопасного и целостного функционирования сети «Интернет», т.е. защите от угроз такому функционированию.

***

Важным нормативным документом высшего уровня, касающимся обеспечения средств противодействия угрозам функционирования ССОП, является Постановление Правительства РФ от 16.03.2009 № 228 (последняя известная редакция от 05.12.2019) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций», включающее в себя утверждение документа «Положение о Федеральной

[4] О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации": Федеральный закон от 01.05.2019 № 90-ФЗ. - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_323815/

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (далее - Положение)[5].

В Положении установлено, что служба по надзору (Роскомнадзор) находится в ведении Министерства цифрового развития, связи и массовых коммуникаций. Согласно Положению, Роскомнадзор осуществляет государственный контроль и надзор в сфере связи, информационных технологий, защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

Служба реализует функции по контролю и надзору в сфере средств массовой информации, в том числе электронных и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы. Служба обеспечивает присвоение и регистрацию радиочастот, лицензирование деятельности в областях связи и выполняет ряд других задач.

В случае возникновения угроз устойчивости, безопасности и целостности функционирования ССОП служба по надзору, в соответствии с требованиями Положения, осуществляет централизованное управление ею путем управления техническими средствами противодействия угрозам и (или) путем передачи обязательных к выполнению указаний операторам связи, собственникам или другим владельцам средств связи, а также их информирование. Для защиты ССОП служба реализует предоставление операторам связи на безвозмездной основе технических средств противодействия угрозам и определяет технические условия их установки.

[5] О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (вместе с "Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций"): Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 30.04.2020). - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_85889/.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

***

Естественным продолжением и конкретизацией мероприятий, предусмотренных Постановлением «О Федеральной службе по надзору в сфере связи…» в части защиты ССОП от угроз, стало Постановление Правительства РФ от 13 февраля 2019 № 136 «О Центре мониторинга и управления сетью связи общего пользования» [6]. Этим Постановлением Федеральная служба по надзору в сфере связи назначается органом, осуществляющим функции по организации создания и функционирования Центра мониторинга и управления сетью связи общего пользования (далее, в пределах настоящего раздела – Центр), а также по организации создания информационной системы мониторинга и управления сетью связи общего пользования.

Реализацией Постановления «О Центре мониторинга…» стал Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31 июля 2019 № 225 «Об утверждении Положения о Центре мониторинга и управления сетью связи общего пользования» [7] с приложением самого этого Положения о Центре. В Положении о Центре определены задачи, функции и порядок его функционирования.

Задачами Центра, в частности, являются организационное и техническое обеспечение выявления угроз функционированию ССОП, информирования причастных сторон и осуществления управления в случае появления таких угроз. Центр участвует в обеспечении предоставления операторам связи технических средств противодействия угрозам и их установки. Центр предоставляет технические условия установки технических средств

[6] О Центре мониторинга и управления сетью связи общего пользования: Постановление Правительства РФ от 13 февраля 2019 г. № 136. - Режим доступа: https://base.garant.ru/72180742/.
[7] Об утверждении Положения о Центре мониторинга и управления сетью связи общего пользования: Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31 июля 2019 г. № 225. - Режим доступа: https://minjust.consultant.ru/documents/44663.

противодействия угрозам устойчивости, безопасности и целостности функционирования сети Интернет и сети связи общего пользования, а также требования к сетям связи при использовании технических средств противодействия угрозам.

Центр взаимодействует с органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности РФ. Согласно Положению, в случае возникновения угроз Центр обеспечивает передачу обязательных к выполнению указаний лицам, участвующим в централизованном управлении, и операторам связи, а также координацию их действий.

***

С целью регулирования отношений, возникающих, в частности, при осуществлении права на передачу информации и обеспечении её защиты, принят Федеральный Закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя известная редакция действует с 13 декабря 2019 г.) [8] . Законом регламентируются правила использования информационно-телекоммуникационных сетей. Для ограничения доступа к сайтам в сети "Интернет", содержащим информацию, распространение которой запрещено, создан реестр соответствующих доменных имен и сетевых адресов. Владельцам информационно-телекоммуникационных сетей запрещается предоставлять возможность доступа к таким информационным ресурсам.

Согласно этому Закону Роскомнадзор осуществляет создание и эксплуатацию информационной системы, содержащей перечень информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен. Соответствующая информация должна быть получена на основании обращения федерального органа исполнительной

[8] Об информации, информационных технологиях и о защите информации: Федеральный Закон от 27 июля 2006 № 149-ФЗ (ред. от 03.04.2020). - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

власти, осуществляющего оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации.

Закон предусматривает принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, блокирования, копирования, а также от иных неправомерных действий в отношении информации. Отдельной статьёй изложены требования о защите информации, содержащейся в государственных информационных системах. Особо отмечено, что федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

***

Для нормативного обеспечения организационно-технических мер безопасности Министерство издало приказ от 27 сентября 2007 № 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования» [9]. В Требованиях сформулированы условия целостности, устойчивости функционирования и живучести ССОП, а также приведены нормы на соответствующие показатели.

Для нормативного обеспечения технических мер противодействия угрозам функционирования ССОП Роскомнадзор издал приказ от 31 июля 2019 г. «Об утверждении технических условий установки технических средств противодействия угрозам, а также требований к сетям связи при использовании технических средств противодействия угрозам» [10]. В Приложениях к Приказу изложены требования к соблюдению

[9]Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования: Приказ Министерства информационных технологий и связи РФ от 27 сентября 2007 № 113. - Режим доступа: https://base.garant.ru/192047/.
[10]Об утверждении технических условий установки технических средств противодействия угрозам, а также требований к сетям связи при использовании технических средств противодействия угрозам: Приказ Роскомнадзора от 31.07.2019 № 228 (зарегистрировано в Минюсте России 11.09.2019 № 55886). - Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_333310/.

соответствующих климатических условий, обеспечению бесперебойного питания, условиям доступа и защиты от несанкционированного доступа к техническим средствам противодействия угрозам, к организации технологического канала связи для управления техническими средствами противодействия угрозам, обладающего пропускной способностью не менее 100 Мбит/с, а также к инфраструктуре сети связи.

Стандарты общего плана (надотраслевые)

Следующими по уровню, но не по важности нормативными документами можно считать стандарты.

Самые общие стандарты, касающиеся управления качеством выпускаемой продукции и/или предоставления услуг, независимо от области деятельности организации (условно – надотраслевые стандарты) – это ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь [1] и ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования [2].

В последних версиях этих стандартов от 2015 г. серьёзное внимание уделяется современным условиям работы предприятий, заметно отличающимся от тех, что были в предыдущие сроки. Отличия эти характеризуются, в частности, ускоренными изменениями, глобализацией рынков, а также появлением новых знаний и технических средств. Устанавливаемый этими стандартами процессный подход усилен в новой версии требованием к «риск-ориентированному мышлению». Деятельность любого предприятия практически всегда включает в себя риски. Такой стиль мышления необходим, поскольку позволяет определять факторы, которые могут привести к отклонению от запланированных результатов, и применить предупреждающие действия для минимизации негативных последствий.

***

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Надотраслевым стандартом, содержащим общие правила управления рисками, является ГОСТ Р ИСО 31000-2019 Менеджмент риска. Принципы и руководство [3] (идентичен международному стандарту ИСО 31000:2018). В разделе «Область применения» подчёркивается, что этот стандарт «*не ограничивается конкретной отраслью или видом деятельности*». Далее утверждается, в частности, что риск-менеджмент способствует обеспечению безопасности и защиты людей.

В стандарте представлена структура менеджмента риска, её необходимые элементы и их взаимосвязь. Риск-менеджмент рассматривается здесь как процесс, включающий в себя следующие этапы: обмен информацией и консультирование; определение области применения, контекста и критериев риска; оценка риска, в том числе его идентификация, анализ и оценивание; воздействие на риск.

В дополнение к стандарту ИСО 31000 разработан ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска [4]. Стандарт, по собственному уведомлению, «*содержит рекомендации по выбору и применению методов оценки риска*». В разделе 4 стандарта приведено разъяснение понятия оценки риска. В разделе 5 описан поэтапно процесс оценки риска. При этом отмечено, что «*при проведении оценки риска может потребоваться применение мультидисциплинарного подхода, так как риски могут попадать в широкий диапазон причин и последствий*». В разделе 6 даны рекомендации по выбору метода оценки риска. В Приложении В стандарта компактно изложены описания 31 метода оценки риска. Каждое описание содержит краткий обзор метода, область применения, входные данные, процесс выполнения, выходные данные, а также его преимущества и недостатки.

Опубликована новая редакция стандарта IEC 31010:2019, которая отличается от предыдущей версии: количество методик оценки риска увеличено до 41, используется другая классификация методик оценки риска,

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

внесены некоторые другие изменения.

Организации, оказывающие услуги электросвязи и причастные к такой деятельности, для целей выявления угроз могут выбрать метод оценки рисков в соответствии с выполняемыми задачами.

Для разработчиков стандартов, относящимся к любым отраслям деятельности, Техническим комитетом по стандартизации ТК 10 «Основополагающие общетехнические стандарты. Оценка эффективности и управление рисками» разработан ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты [5].

В разделе «Область применения» данного стандарта указано, что он «*может быть применен к любым аспектам безопасности, относящимся к людям или имуществу, или окружающей среде, или к сочетанию этих сторон. Правила… основаны на уменьшении риска, возникающего при использовании продукции, процессов или услуг. Стандарт рассматривает полный жизненный цикл продукции, процесса или услуги…*».

Стандарты отраслевые

Документом, устанавливающим основные термины, касающиеся отрасли связи, является ГОСТ Р 53801-2010 Связь федеральная. Термины и определения [6]. Установленные стандартом термины рекомендуется использовать в официальной документации, а также в научной, учебной и справочной литературе.

Для адресного нормативного обеспечения менеджмента качества услуг электросвязи в части защиты от информационных угроз приказом Федерального агентства по техническому регулированию и метрологии утверждён ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения [7]. В разделе «Область применения» документа указано: «*Настоящий стандарт предназначен для применения расположенными на территории Российской Федерации*

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

организациями,… которые связаны с созданием и эксплуатацией сетей электросвязи, являющимися составными компонентами сети связи общего пользования единой сети электросвязи Российской Федерации».

В разделе «Основные положения…» формулируются основные цели и задачи обеспечения безопасности сетей электросвязи, приведено описание показателей вероятности возникновения угроз. В разделе стандарта «Общие требования к безопасности сетей электросвязи» подчёркнуто, что для обеспечения безопасности на каждой стадии жизненного цикла сетей электросвязи должна осуществляться деятельность по поддержанию управления рисками на основе анализа уязвимостей сетей электросвязи и угроз, способных реализовать эти уязвимости.

Стандартом устанавливаются основные мероприятия по обеспечению безопасности сетей электросвязи и положения о структуре системы её обеспечения. Отмечено, что «*система обеспечения безопасности (СОБ) сетей электросвязи ССОП является элементом системы информационной безопасности Российской Федерации… и состоит из взаимодействующих между собой служб обеспечения безопасности различных операторов связи, координируемых центральным органом СОБ*».

Тематически со стандартом ГОСТ Р 52448-2005 тесно связаны стандарты ГОСТ Р 53109, ГОСТ Р 53110 и ГОСТ Р 53111.

Документ ГОСТ Р 53110-2008 Система обеспечения информационной безопасности сети связи общего пользования. Общие положения [8] «*определяет правовые, организационные и технические направления обеспечения информационной безопасности сетей электросвязи, входящих в состав сети связи общего пользования*». В стандарте определены объект и субъект информационной безопасности сети электросвязи, под которой понимается «*способность сети электросвязи противостоять преднамеренным и непреднамеренным дестабилизирующим воздействиям (угрозам безопасности) на входящие в состав сети средства и линии связи в*

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

процессе приема и передачи, обработки и хранения информации, что может привести к ухудшению качества услуг, предоставляемых сетью электросвязи». Стандарт требует, чтобы в каждой организации связи оператором были организованы система обеспечения информационной безопасности (СОИБ) и система менеджмента информационной безопасности.

В стандарте описаны жизненный цикл СОИБ, его взаимосвязь с жизненным циклом сети связи, а также архитектура этой системы; изложено требование о создании в организации связи соответствующей организационно-штатной структуры (служба, подразделение или администратор), осуществляющей выполнение мероприятий по обеспечению безопасности ИБ сети электросвязи.

Стандарт ГОСТ Р 53111-2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки [9] «устанавливает требования к устойчивости функционирования сетей электросвязи, входящих в состав сети связи общего пользования».

В разделе «Основные положения по обеспечению устойчивости функционирования сетей электросвязи» рассмотрено воздействие внутренних и внешних дестабилизирующих факторов (ДФ) на сети электросвязи. В нём далее указаны наиболее распространённые источники ДФ, классификация их в зависимости от характера воздействия на элементы сети, по природе возникновения и по ряду других признаков; подчёркнут их вероятностный характер.

В разделе приведена оценка ущерба, наносимого сети электросвязи воздействием ДФ, в том числе провоцируемых чрезвычайными ситуациями. Приводятся градации уровней ущерба сети электросвязи, а также методы оценки устойчивости и уязвимости объектов электросвязи по различным признакам.

В Приложение А «Перечень требований к устойчивости

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

функционирования сети электросвязи» установлены показатели, характеризующие устойчивость функционирования сети электросвязи и требования к их значениям.

Стандарт ГОСТ Р 53109-2008 Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности [10] «*устанавливает требования к форме и содержанию паспорта организации связи по информационной безопасности относительно сети (сетей) электросвязи*».

Стандартом определено, что «*паспортизации по требованиям к информационной безопасности подлежат все организации связи,… функционирующие как… комплекс, предназначенный для оказания услуг связи, предоставляемых с использованием сети связи общего пользования*». В стандарте допускается, что форма и содержание паспортов в разных организациях могут быть различными. Вместе с тем, указано, что сведения, включенные в паспорт, должны периодически уточняться и обновляться.

В стандарте изложен порядок составления паспорта по информационной безопасности организации и даны рекомендации по его ведению. В приложении А приведен пример формы паспорта организации связи по информационной безопасности. В приложениях Б и В рекомендованы порядок установления категории сетей по защите от несанкционированного доступа и образец акта о категорировании.

Стандарты межотраслевые

Отрасль электросвязи существует не изолированно от других видов деятельности. Организации, занимающиеся созданием и эксплуатацией сетей или предоставлением услуг электросвязи, должны поэтому выполнять требования нормативных документов, не адресованных им непосредственно, но затрагивающих отдельные проблемы, касающиеся этих организаций. Некоторые из таких межотраслевых стандартов способствуют, в частности,

противодействию угрозам устойчивому функционированию сети связи общего пользования.

Поскольку основу современного оборудования электросвязи составляют электронные устройства, при их разработке, монтаже и эксплуатации должны выполняться общие для всех отраслей требования (ГОСТы), касающиеся электропитания (включая бесперебойное), заземления оборудования, а также электромагнитной совместимости технических средств. Анализ таких стандартов требует отдельного рассмотрения; здесь приведены лишь выборочные примеры [11-16]. Намеренное и ненамеренное неисполнение требований таких стандартов представляет явную угрозу работе оборудования сети.

Сети электросвязи предназначены для транспортировки информации пользователей. Вместе с тем, значительную часть оборудования самих этих сетей (коммутационные и биллинговые системы, колл-центры, системы мониторинга и управления и др.) составляют программно-аппаратные комплексы, осуществляющие сбор, обработку и хранение информации. На эти комплексы распространяются требования многих стандартов, касающихся информационных технологий, методов обеспечения безопасности и защиты информации.

Среди этих документов – группа стандартов ГОСТ Р ИСО/МЭК 13335 Информационная технология. Методы и средства обеспечения безопасности, включающая части 1-5 [17-21]. Определённый интерес представляет Часть 1. «Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий», непосредственно затрагивающая сети электросвязи.

Важной для противодействия угрозам ССОП следует признать группу стандартов ГОСТ Р 53113. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

каналов. Часть 1. Общие положения [22] и ГОСТ Р 53113. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов [23].

Стандарты эти актуальны уже потому, например, что цифровые управляющие подсистемы практически всех систем коммутации (телефонных станций и т.п.) по заявлениям изготовителей имеют доступ для возможности дистанционного контроля и управления из множества точек всемирной сети электросвязи. Таким образом, для таких систем существует угроза несанкционированного вмешательства в работу вплоть до полного их отключения.

Утверждена и введена в действие серия стандартов ГОСТ Р ИСО/МЭК 27ххх Информационная технология. Методы и средства обеспечения безопасности [24-39]. В состав серии вошло 17 стандартов (предполагается, что она может быть расширена). Среди стандартов серии – ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. На него имеются ссылки как на основной во многих других стандартах серии. Кроме того, следует отметить ГОСТ Р ИСО/МЭК 27011-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002, затрагивающий проблемы защиты от угроз сетей электросвязи.

Для оценки безопасности информационных технологий, применяемых в электросвязи, необходимо следовать правилам, изложенным в группе стандартов ГОСТ Р ИСО/МЭК 15408 Информационная технология (ИТ).

Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий:

- Часть 1. Введение и общая модель;
- Часть 2. Функциональные компоненты безопасности;
- Часть 3. Компоненты доверия к безопасности [40-42].

***

Федеральным агентством по техническому регулированию и метрологии утверждена система стандартов по защите (некриптографическими методами) информации [43-48]. На сетях электросвязи, в том числе и ССОП, в защите нуждается как информация пользователей (влияет на показатели качества предоставляемых услуг электросвязи), так и собственная внутренняя информация (влияет на надёжность, живучесть, устойчивость функционирования сети и т.п.).

Организации, деятельность которых связана с проектированием, монтажом и эксплуатацией сети связи общего пользования и предоставлением услуг электросвязи, обязаны выполнять требования указанных стандартов.

Основные выводы

Настоящий обзор, не претендующий на исчерпывающую полноту, позволяет сделать выводы, следующие ниже.

1. Нормативное обеспечение средств противодействия угрозам ССОП – это широко развитая система документов разных уровней, от федеральных законов и постановлений Правительства до стандартов, регулирующих деятельность организаций, влияющих на качество услуг электросвязи.

2. Неизбежный прогресс в развитии глобальной сети электросвязи, усложнение средств и услуг электросвязи, появление новых или более строгих требований к содержанию и качеству этих услуг со стороны

надзирающих органов и потребителей – всё это влечёт необходимость совершенствования существующей нормативной документации и создания новых документов, что и наблюдается в действительности.

3. Организации и предприятия, которые связаны с созданием и эксплуатацией сетей электросвязи, либо причастны к обеспечению безопасности функционирования этих сетей, должны постоянно осуществлять мониторинг и анализ соответствующей нормативной документации для своевременного выполнения её требований в своей деятельности.

Список литературы

1. Системы менеджмента качества. Основные положения и словарь: ГОСТ Р ИСО 9000-2015. - М.: Стандартинформ, 2019. - 53 с.

2. Системы менеджмента качества. Требования: ГОСТ Р ИСО 9001. - М.: Стандартинформ, 2015. - 28 с.

3. Менеджмент риска. Принципы и руководство: ГОСТ Р ИСО 31000-2019. - М.: Стандартинформ, 2020. - 14 с.

4. Менеджмент риска. Методы оценки риска: ГОСТ Р ИСО/МЭК 31010-2011. - М.: Стандартинформ, 2012. - 70 с.

5. Аспекты безопасности. Правила включения в стандарты: ГОСТ Р 51898-2002. - М.: Стандартинформ, 2002. - 6 с.

6. Связь федеральная. Термины и определения: ГОСТ Р 53801-2010. - М.: Стандартинформ, 2011. - 26 с.

7. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения: ГОСТ Р 52448-2005. - М.: Стандартинформ, 2006. - 16 с.

8. Система обеспечения информационной безопасности сети связи общего пользования. Общие положения: ГОСТ Р 53110-2008. - М.: Стандартинформ, 2009. - 20 с.

9. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки: ГОСТ Р 53111-2008. - М.: Стандартинформ, 2009. - 16 с.

10. Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности: ГОСТ Р 53109-2008. - М.: Стандартинформ, 2009. - 15 с.

11. Совместимость технических средств электромагнитная. Термины и определения: ГОСТ 30372 (IEC 60050-161:1990). - М.: Стандартинформ, 2018. - 59 с.

12. Совместимость технических средств электромагнитная. Устойчивость к кондуктивным помехам, наведенным радиочастотными электромагнитными полями. Требования и методы испытаний: ГОСТ Р 51317.4.6 (МЭК 61000-4-6-96). - М.: Госстандарт России, 2000. - 30 с.

13. Совместимость технических средств электромагнитная. Устойчивость к провалам, кратковременным прерываниям и изменениям напряжения электропитания. Требования и методы испытаний: ГОСТ 30804.4.11 (IEC 61000-4-11:2004) - М.: Стандартинформ, 2014. - 21 с.

14. Совместимость технических средств электромагнитная. Устойчивость к наносекундным импульсным помехам. Требования и методы испытаний: ГОСТ 30804.4.4 (IEC 61000-4-4:2004). - М.: Стандартинформ, 2014. - 22 с.

15. Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения: ГОСТ 32144. - М.: Стандартинформ, 2014. - 16 с.

16. Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования: ГОСТ Р 52863-2007. - М.: Стандартинформ, 2008. - 34 с.

17. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий: ГОСТ Р ИСО/МЭК 13335-1 - 2006. - М.: Стандартинформ, 2007. - 18 с.

18. Информационная технология. Методы и средства обеспечения безопасности. Часть 2. Управление и планирование защиты IT: ГОСТ Р ИСО/МЭК 13335-2. - М.: Стандартинформ, 2002.

19. Информационная технология Методы и средства обеспечения безопасности. Часть 3 Методы менеджмента безопасности информационных технологий: ГОСТ Р ИСО/МЭК ТО 13335-3-2007. - М.: Стандартинформ, 2007. - 46 с.

20. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер: ГОСТ Р ИСО/МЭК ТО 13335-4-2007. - М.: Стандартинформ, 2002. - 61 с.

21. Информационная технология. Методы и средства обеспечения безопасности. Часть 5 Руководство по менеджменту безопасности сети: ГОСТ Р ИСО/МЭК ТО 13335-5-2006. - М.: Стандартинформ, 2002. - 22 с.

22. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения: ГОСТ Р 53113.1-2008. М.: Стандартинформ, 2009. - 8 с.

23. Информационная технология (ИТ). Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов: ГОСТ Р 53113.2-2009. - М.: Стандартинформ, 2010. - 8 с.

24. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Требования: ГОСТ Р ИСО/МЭК 27001-2006. - М.: Стандартинформ, 2008. - 26 с.

25. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности: ГОСТ Р ИСО/МЭК 27002-2012. - М.: Стандартинформ, 2014. - 96 с.

26. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности: ГОСТ Р ИСО/МЭК 27003-2012. - М.: Стандартинформ, 2014. - 54 с.

27. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения: ГОСТ Р ИСО/МЭК 27004-2011. - М.: Стандартинформ, 2012. - 55 с.

28. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности: ГОСТ Р ИСО/МЭК 27005-2010. - М.: Стандартинформ, 2011. - 47 с.

29. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности: ГОСТ Р ИСО/МЭК 27006-2008. - М.: Стандартинформ, 2010. - 36 с.

30. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности: ГОСТ Р ИСО/МЭК 27007-2014. - М.: Стандартинформ, 2019. - 24 с.

31. Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью. ГОСТ Р 56045-2014/ISO/IEC TR 27008:2011. - М.: Стандартинформ, 2015. - 40 с.

32. Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002: ГОСТ Р ИСО/МЭК 27011-2012. - М.: Стандартинформ, 2014. - 92 с.

33. Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1: ГОСТ Р ИСО/МЭК 27013-2014. - М.: Стандартинформ, 2014. - 44 с.

34. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса: ГОСТ Р ИСО/МЭК 27031-2012. - М.: Стандартинформ, 2014. - 56 с.

35. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции: ГОСТ Р ИСО/МЭК 27033-1-2011. - М.: Стандартинформ, 2012. - 66 с.

36. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления: ГОСТ Р ИСО/МЭК 27033-3-2014. - М.: Стандартинформ, 2019. - 26 с.

37. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия: ГОСТ Р ИСО/МЭК 27034-1-2014. - М.: Стандартинформ, 2015. - 64 с.

38. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме: ГОСТ Р ИСО/МЭК 27037-2014. - М.: Стандартинформ, 2014. - 41 с.

39. Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования: ГОСТ Р ИСО/МЭК 27038-2016. - М.: Стандартинформ, 2016. - 10 с.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

40. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель: ГОСТ Р ИСО/МЭК 15408-1-2012. - М.: Стандартинформ, 2014. - 50 с.

41. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности: ГОСТ Р ИСО/МЭК 15408-2-2013. - М.: Стандартинформ, 2014. - 156 с.

42. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности: ГОСТ Р ИСО/МЭК 15408-3-2013. - М.: Стандартинформ, 2014. - 267 с.

43. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006. - М.: Стандартинформ, 2006. - 8 с.

44. Защита информации. Объекты информатизации. Факторы, воздействующие на информацию. Общие положения: ГОСТ Р 51275-2006. - М.: Стандартинформ, 2018. - 7 с.

45. Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения: ГОСТ Р 51624-2000. - М.: Госстандарт России, 2000. - 14 с.

46. Защита информации. Система стандартов. Основные положения: ГОСТ Р 52069.0-2013. - М.: Стандартинформ, 2014. - 12 с.

47. Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования: ГОСТ Р 52863-2007. - М.: Стандартинформ, 2008. - 33 с.

48. Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

преднамеренных силовых электромагнитных воздействий. Общие положения: ГОСТ Р 56103-2014. - М.: Стандартинформ, 2015. - 18 с.

Regulatory Provision of Means of Counteracting Threats of Public Communication Network - Factor of Influence on Management of Quality of Telecommunication Services

Vaynzof Leonid Abramovich,

Candidate of Technical Sciences,

Specialist of Quality Systems Certification Center "Interecoms"

Normative provision of means of counteracting threats of the public communication network (SSOP) is a widely developed system of documents of different levels. The inevitable progress in the development of the global telecommunication network, the complication of telecommunication facilities and services, the emergence of new or stricter requirements for the content and quality of these services by supervisory bodies and consumers - all this leads to the need to improve existing regulatory documents and create new documents.

Organizations and enterprises connected with the creation and operation of telecommunication networks or involved in ensuring the safety of these networks should constantly monitor and analyze the relevant regulatory documentation in order to meet its requirements in a timely manner in their activities.

The article analyses federal legislation establishing the basis of communication activities in the territory of the Russian Federation, as well as industry and industry standards related to telecommunication services in the field of protection against information threats.

Keywords: telecommunication network, telecommunication services, public communication networks, safety of telecommunication networks operation, countering threats of public communication network, regulatory support, regulatory documentation, standards, quality management.