

Требования по защите сетей связи от несанкционированного доступа и передаваемой по ним информации

Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации принят приказ, утверждающий требования по защите сетей связи от несанкционированного доступа и передаваемой по ним информации [1].

Проект приказа был внесен Минкомсвязи РФ 27 декабря 2017 г для оценки регулирующего воздействия. По результатам обсуждений и экспертизы проект приказа с учетом доработок получил положительное заключение об оценке регулирующего воздействия (Заключение Минэкономразвития об ОРВ № 15354-СШ/Д26и от 05.06.2018). Минэкономразвитием России сделан вывод об отсутствии в проекте акта положений, вводящих избыточные обязанности, запреты и ограничения для физических и юридических лиц в сфере предпринимательской и иной экономической деятельности или способствующих их введению, а также положений, приводящих к возникновению необоснованных расходов физических и юридических лиц в сфере предпринимательской и иной экономической деятельности, а также бюджетов всех уровней бюджетной системы Российской Федерации.

Приказ принят в рамках требования Федерального закона "О связи" [2], по которому Минкомсвязи необходимо установить требования по защите сетей связи от несанкционированного доступа к ним и передаваемой по ним информации, порядку ввода сетей связи в эксплуатацию.

Принятый приказ признает не подлежащим применению, действующий с 2008 года аналогичный приказ Министерства информационных технологий и связи Российской Федерации с требованиями по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации [3].

Принятые Требования распространяются на сети электросвязи, входящие в состав сети связи общего пользования, за исключением сетей связи для трансляции телеканалов и (или) радиоканалов. Напомним, что сеть связи общего пользования:

- предназначена для возмездного оказания услуг электросвязи любому пользователю услугами связи на территории Российской Федерации;
- включает в себя сети электросвязи, определяемые географически в пределах обслуживаемой территории и ресурса нумерации и не определяемые географически в пределах территории Российской Федерации и ресурса нумерации, а также сети связи, определяемые по технологии реализации оказания услуг связи.

Новым приказом предусмотрены следующие требования:

Меры защиты

Операторы связи должны принимать меры в целях защиты от несанкционированного доступа к сетям связи и передаваемой по ним информации. К таким мерам Требованиями отнесены **организационные и технические** меры. Принимаемые меры должны быть направлены на предотвращение доступа к линиям связи, сооружениям связи, средствам связи, находящимся как внутри, так и вне сооружений связи, и передаваемой по сетям связи информации, осуществляемого с нарушением установленного этими операторами связи порядка доступа. Порядок доступа устанавливается и утверждается операторами связи.

Категорирование узлов связи по защищенности

Требованиями установлено, что узлы связи сетей связи должны подразделяться на узлы связи I, II, III категории защищенности. Категорирование узлов связи по защищенности проводится исходя из следующих параметров:

- типа сети (- Сети фиксированной телефонной связи, - Сети подвижной радиосвязи, сети подвижной радиотелефонной связи, сети подвижной спутниковой радиосвязи, - Сети передачи данных, - Сети телеграфной связи).
- типа узла (- узлы связи сетей междугородной и международной телефонной связи, сетей зоновой телефонной связи, узлы связи сетей местной телефонной связи)
- емкости узла (- с количеством портов более 10000, - от 1024 до 10000, - до 1024, - емкостью свыше 500 Гбит в секунду, - свыше 100 Гбит и менее 500 Гбит в секунду, - менее 100 Гбит в секунду).

Требования по защите

Требования по защите установлены в зависимости от средств, подлежащих защите:

- а) Для защиты узлов связи сетей фиксированной телефонной связи, сетей подвижной радиосвязи, сетей подвижной радиотелефонной связи, сетей подвижной спутниковой радиосвязи, сетей передачи данных, сетей телеграфной связи.
- б) Для защиты от несанкционированного доступа к программным средствам узлов связи сетей фиксированной телефонной связи, сетей подвижной радиосвязи, сетей подвижной радиотелефонной связи, сетей подвижной спутниковой радиосвязи, сетей передачи данных, сетей телеграфной связи.
- в) Для защиты от несанкционированного доступа к средствам связи, не входящим в состав узлов связи сетей фиксированной телефонной связи, сетей подвижной радиосвязи, сетей подвижной радиотелефонной связи, сетей подвижной спутниковой радиосвязи, сетей передачи данных, сетей телеграфной связи.
- г) Для защиты от несанкционированного доступа к линиям связи, соединяющим узлы связи сетей фиксированной телефонной связи, сетей подвижной радиосвязи, сетей подвижной радиотелефонной связи, сетей подвижной спутниковой радиосвязи, сетей передачи данных, сетей телеграфной связи.
- д) Для защиты от несанкционированного доступа к абонентским линиям связи сетей фиксированной телефонной связи, сетей телеграфной связи, сетей передачи данных.
- е) Для повышения защищенности сетей связи от несанкционированного доступа к программным средствам и программно-аппаратным комплексам средств связи, осуществляемого дистанционно.
- ж) Для защиты от несанкционированного доступа к информации, передаваемой посредством сетей подвижной радиосвязи, сетей подвижной радиотелефонной связи, сетей подвижной спутниковой радиосвязи.

Для защиты от несанкционированного доступа к информации, передаваемой посредством сетей подвижной радиосвязи, сетей подвижной радиотелефонной связи, сетей подвижной спутниковой радиосвязи, установлено, что операторы связи должны обеспечивать реализацию процедур аутентификации и идентификации абонентов **с использованием средств криптографической защиты информации, удостоверяемых сертификатами соответствия требованиям федерального органа исполнительной власти в области обеспечения безопасности** к шифровальным (криптографическим) средствам класса КА для оборудования коммутации узлов связи и класса КСЗ для модуля идентификации абонентов USIM (R-UI) в составе абонентского оборудования.

Так же, в случае обнаружения признаков компьютерной атаки на средства связи оператора связи, а также средства связи иных операторов связи при пропуске трафика, Оператор связи должен предпринимать меры по защите сетей и средств связи в соответствии с порядком, установленным оператором связи и действующими нормативными актами.

Факт обнаружения признаков компьютерной атаки должен регистрироваться оператором связи в электронном или ином виде, пригодном для последующей обработки и анализа.

События, связанные с несанкционированным доступом к сетям связи и передаваемой по ним информации должны регистрироваться в электронном или ином виде, пригодном для последующей обработки и анализа.

Исполнение вводимых Требований проверяется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами при проведении плановых проверок при осуществлении федерального государственного надзора в области связи. При проведении проверок проверяется, обеспечивается ли оператором связи при построении и эксплуатации сетей связи защита средств и сооружений связи от несанкционированного доступа к ним и передаваемой посредством их информации. В результате проводимых Управлениями Роскомнадзора плановых выездных проверок устанавливается, что оператор не выполняет требования по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации: не осуществляется осмотр линий связи в соответствии с порядком, установленным оператором связи, не ведется журнал осмотра, не обеспечивается размещение линий связи в специальных коробах и распределительных коробках, оснащенных запирающими устройствами. Это является нарушением установленных требований и наказывается административным производством по ч. 3 ст. 14.1 КоАП РФ.

По состоянию на 15 августа Приказ [1] возвращен без государственной регистрации Минюстом России (Письмо Минюста РФ от 31.07.2018 N 01/101160-ДН). Текст приказа официально не опубликован.

Согласно ст. 8 и 10 Указа Президента РФ от 23.05.96 № 763 нормативные правовые акты федеральных органов исполнительной власти, которые должны пройти процедуру государственной регистрации в Минюсте России, подлежат обязательному официальному опубликованию. Нормативные правовые акты федеральных органов исполнительной власти, не прошедшие государственную регистрацию, не влекут правовых последствий как не вступившие в силу и не служат основанием для регулирования соответствующих правоотношений. Постановление Правительства РФ от 13.08.97 № 1009 детально регулирует порядок подготовки нормативных правовых актов федеральными органами исполнительной власти, условия, при которых они подлежат государственной регистрации

в Минюсте России, порядок их опубликования и вступления в силу. Так, нормативные правовые акты, подлежащие государственной регистрации, исполняются только после их регистрации и официального опубликования (п. 19 Правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации).

[1] - Приказ Минкомсвязи России от 25.06.2018 N 318 "Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой по ним информации".

[2] - Федеральный закон "О связи" от 07.07.2003 N 126-ФЗ.

[3] - приказ Министерства информационных технологий и связи Российской Федерации от 09.01.2008 № 1 "Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации".