

**УТВЕРЖДЕНЫ**

Приказом Министерства связи  
Донецкой Народной  
Республики  
от \_\_\_\_\_ 2018 года № \_\_\_\_

## **ПРАВИЛА**

### **по защите телекоммуникационных сетей Донецкой Народной Республики от несанкционированного доступа к ним и передаваемой по ним информации**

#### **I. Общие положения**

1.1. Настоящие Правила по защите телекоммуникационных сетей Донецкой Народной Республики от несанкционированного доступа к ним и передаваемой по ним информации (далее — Правила) разработаны, руководствуясь частью 1 статьи 8 Закона Донецкой Народной Республики «О телекоммуникациях», пунктами 15.2.3, 15.4 Временного Положения о Министерстве связи Донецкой Народной Республики, утвержденного Постановлением Совета Министров Донецкой Народной Республики от 10.01.2015 № 1-17.

1.2. В настоящих Правилах термины и понятия используются в соответствии с законодательством Донецкой Народной Республики в сфере телекоммуникаций.

1.3. Настоящие Правила разработаны в целях защиты телекоммуникационных сетей от несанкционированного доступа к ним и передаваемой по ним информации.

1.4. Настоящие Правила распространяются на телекоммуникационные сети, входящие в состав телекоммуникационной сети общего пользования, за исключением телекоммуникационных сетей для распространения программ эфирного телевизионного вещания и радиовещания.

1.5. В целях защиты от несанкционированного доступа к телекоммуникационным сетям и передаваемой по ним информации операторы телекоммуникаций самостоятельно устанавливают порядок доступа к линиям связи, сооружениям телекоммуникаций, средствам телекоммуникаций, находящимся как внутри, так и вне сооружений телекоммуникаций, и передаваемой по ним информации, (далее — порядок доступа), с описанием

соответствующих организационных и технических мер, направленных на реализацию порядка доступа.

Лица, нарушившие порядок доступа, несут ответственность в соответствии с законодательством Донецкой Народной Республики.

1.6. Порядок доступа утверждается уполномоченным лицом оператора телекоммуникаций и включает:

1.6.1. описание организации пропускного режима на охраняемую территорию, в пределах которой размещаются сооружения телекоммуникаций (далее – охраняемая территория), и порядок охраны этой территории;

1.6.2. описание процедур применения на охраняемой территории инженерных средств защиты, технических средств обнаружения и сигнализации;

1.6.3. установление перечня и образцов документов, дающих право находиться в охраняемой зоне, а также в сооружениях телекоммуникаций и отдельных помещениях, расположенных в пределах охраняемой территории;

1.6.4. организационные процедуры оформления допуска к проведению работ на средствах телекоммуникаций и линиях связи, а также работ, связанных с технологической возможностью доступа к информации, передаваемой посредством телекоммуникационной сети, и установление списка лиц, имеющих право на проведение таких работ;

1.6.5. описание процедур регистрации событий, связанных с осуществлением доступа к средствам телекоммуникаций, линиям связи и сооружениям телекоммуникаций.

1.7. Телекоммуникационные узлы телекоммуникационных сетей подразделяются на телекоммуникационные узлы I, II, III категории защищенности. Категорирование телекоммуникационных узлов по защищенности приведено в Приложении к настоящим Правилам.

## **II. Требования по защите от несанкционированного доступа к средствам телекоммуникаций и линиям связи телекоммуникационных сетей и передаваемой по ним информации**

2.1. Для защиты телекоммуникационных сетей от физического доступа со стороны лиц, не имеющих на это права, операторам телекоммуникаций необходимо обеспечивать:

2.1.1. оснащение сооружений телекоммуникаций, в которых размещаются телекоммуникационные узлы, в том числе, телекоммуникационные узлы I категории защищенности, средствами контроля доступа, инженерной защиты и техническими средствами охранной сигнализации;

2.1.2. наличие средств инженерной защиты, препятствующих несанкционированному проходу и (или) въезду лиц и (или) транспорта на охраняемую территорию для телекоммуникационных узлов I и II категории защищенности;

2.1.3. организацию охраны телекоммуникационных узлов I и II категории защищенности;

2.1.4. организацию контрольно-пропускного режима как на охраняемой территории, так и внутри сооружений телекоммуникаций, в которых размещаются телекоммуникационные узлы I и II категории защищенности;

2.1.5. наличие запирающих устройств для помещений, в которых размещены узлы связи III категории защищенности.

2.2. Для защиты от несанкционированного доступа к программным средствам телекоммуникационных узлов телекоммуникационных сетей операторам телекоммуникаций необходимо обеспечивать:

2.2.1. принятие мер, исключающих возможность доступа к телекоммуникационным сетям лиц, не имеющих на это права, и (или) нарушающих установленный оператором телекоммуникаций порядок доступа к телекоммуникационным сетям;

2.2.2. контроль за подключением в телекоммуникационных узлах технических и программных средств, используемых в процессе обслуживания и эксплуатации телекоммуникационных узлов;

2.2.3. регистрацию и последующий контроль доступа обслуживающего персонала в процессе обслуживания и эксплуатации телекоммуникационных узлов в соответствии с установленным порядком доступа к средствам телекоммуникаций и линиям связи;

2.2.4. разграничение прав доступа, в том числе использование обслуживающим персоналом идентификационных и (или) аутентификационных кодов для телекоммуникационных узлов I и II категории защищенности;

2.2.5. регистрацию и последующий контроль фактов доступа к средствам телекоммуникаций и линиям связи в процессе эксплуатации телекоммуникационных узлов I и II категории защищенности;

2.2.6. применение процедуры идентификации потребительского (оконечного) оборудования в сетях подвижной радиосвязи, сетях подвижной (мобильной) связи, сетях подвижной спутниковой радиосвязи и сетях передачи данных;

2.2.7. установление процедур аутентификации обслуживающего персонала при удаленном доступе к телекоммуникационным узлам I категории защищенности.

2.3. Для защиты от несанкционированного доступа к средствам телекоммуникаций, не входящим в состав телекоммуникационных узлов телекоммуникационных сетей операторам телекоммуникаций необходимо обеспечивать:

2.3.1. оснащение контейнеров, в которых размещено телекоммуникационное оборудование, находящееся вне сооружений телекоммуникаций, средствами инженерной защиты и охранной сигнализации и (или) средствами контроля доступа;

2.3.2. по возможности, оснащение распределительных устройств средствами инженерной защиты и охранной сигнализации и (или) средствами контроля доступа;

2.3.3. по возможности, оборудование распределительных кабельных шкафов запирающими устройствами и датчиками охранной сигнализации;

2.3.4. периодический осмотр антенно-мачтовых сооружений, линейно-кабельных сооружений, в том числе колодцев кабельной канализации, оконечных кабельных устройств, размещенных в распределительных шкафах и коробках в соответствии с порядком, установленным оператором телекоммуникаций, и ведение журнала осмотра.

2.4. Для защиты от несанкционированного доступа к линиям связи, соединяющим телекоммуникационные узлы телекоммуникационных сетей операторам телекоммуникаций необходимо обеспечивать:

2.4.1. установление охранных зон в соответствии с Постановлением Совета Министров Донецкой Народной Республики от 10 марта 2017 года № 3-

28 «Об утверждении Правил охраны сооружений и линий связи в Донецкой Народной Республике»;

2.4.2. осмотр линий связи, проводимый в соответствии с порядком, установленным оператором телекоммуникаций, и ведение журнала осмотра;

2.4.3. применение мер организационного и (или) технического характера по обнаружению несанкционированного подключения к проводным линиям связи;

2.4.4. кодирование сигналов в радиоканалах при применении радиоэлектронных средств;

2.4.5. размещение линий связи, затрудняющее возможность доступа к ним без использования каких-либо инструментов или механизмов.

2.5. Для защиты от несанкционированного доступа к абонентским линиям телекоммуникационных сетей местной телефонной связи, телекоммуникационных сетей передачи данных, телекоммуникационных сетей телеграфной связи операторам телекоммуникаций необходимо обеспечивать:

2.5.1. размещение линий связи в специальных электротехнических коробах или внутри стен зданий, строений, или размещение линий связи, исключающее или затрудняющее возможность доступа к ним без использования каких-либо инструментов или механизмов;

2.5.2. осмотр линий связи, проводимый в соответствии с порядком, установленным оператором телекоммуникаций.

2.6. Защита от несанкционированного доступа к абонентским линиям при применении радиоэлектронных средств обеспечивается кодированием информации в радиоканале.

### **III. Требования к контролю и регистрации событий, связанных с несанкционированным доступом к телекоммуникационным сетям и передаваемой по ним информации**

3.1. События, связанные с несанкционированным доступом к телекоммуникационным сетям и передаваемой по ним информации (далее – события), регистрируются документально и заверяются подписью должностного лица оператора телекоммуникаций, зарегистрировавшего это событие.

Регистрационная запись события содержит:

3.1.1. указание на средство телекоммуникаций или линию связи, к которым был осуществлен несанкционированный доступ и условное (кодовое) обозначение события;

3.1.2. описание события;

3.1.3. описание последствия события;

3.1.4. дату и время события и (или) регистрации события;

3.1.5. указание на лицо, выявившее событие.

3.2. В целях предотвращения возникновения событий, связанных с несанкционированным доступом к телекоммуникационным сетям и к передаваемой по ним информации, в процессе эксплуатации телекоммуникационных сетей операторами телекоммуникаций проводится анализ выявленных событий, причин и условий их возникновения. По результатам такого анализа составляются заключение и план-график работ, направленных на предотвращение возникновения в дальнейшем событий, связанных с несанкционированным доступом к телекоммуникационным сетям.

Результаты работ, проведенных в соответствии с планом-графиком, отражаются в соответствующих эксплуатационных документах.

**Начальник отдела государственного  
регулирования услуг передачи данных**

**В.А. Яркошенко**

### Категорирование телекоммуникационных узлов по защищенности

Категории	I	II	III
Типы сетей			
Сети телефонной связи	узлы связи сетей международной телефонной связи, узлы связи сетей местной телефонной связи с емкостью телефонной сети более 10000 номеров, а также транзитные и оконечно-транзитные телекоммуникационные узлы сетей местной телефонной связи, которые соединяются с узлами обслуживания вызовов экстренных оперативных служб	телекоммуникационные узлы сети местной телефонной связи с емкостью телефонной сети от 1024 до 10000 номеров, за исключением транзитных и оконечно-транзитных телекоммуникационных узлов, которые соединяются с узлами обслуживания вызовов экстренных оперативных служб	телекоммуникационные узлы сети местной телефонной связи с емкостью телефонной сети до 1024 номеров
Сети подвижной радиосвязи, сетей подвижной (мобильной) связи, сетей подвижной спутниковой радиосвязи	телекоммуникационные узлы сети подвижной радиосвязи, сетей подвижной (мобильной) связи, телекоммуникационные узлы в составе наземных станций сопряжения сети подвижной спутниковой радиосвязи	—	—
Сети передачи данных	международные транзитные телекоммуникационные узлы	транзитные телекоммуникационные узлы	оконечные телекоммуникационные узлы, оконечно-транзитные телекоммуникационные узлы
Сети телеграфной связи	международные телекоммуникационные узлы	—	зоновые телекоммуникационные узлы