ВВЕДЕНЫ В ДЕЙСТВИЕ
для опытного использования в тестовом режиме
решением Исполкома Общественно-
государственного объединения
«Ассоциация документальной электросвязи»
от 26 июня 2019г.

СОГЛАСОВАНО 8 Центр ФСБ России (исх. № 149/2/7- 370 от « 5 » апреля 2019г.)	СОГЛАСОВАНО Общественно-государственное объединение «Ассоциация документальной электросвязи» (протокол от 27 марта 2019г.)	СОГЛАСОВАНО ФСТЭК России (исх. № 240/25/1221 от « 18 » марта 2019г.)

Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи

Москва
2019

Аннотация

Настоящий документ разработан на базе материалов от операторов связи, оказывающих услуги подвижной радиосвязи в сети связи общего пользования, и содержит методические рекомендации по категорированию объектов критической информационной инфраструктуры актуальные для большинства операторов связи, оказывающих услуги связи в сети связи общего пользования.

Настоящий документ не распространяется на объекты критической информационной инфраструктуры, используемые для оказания услуг операторами выделенных сетей связи, объекты, входящие в состав и/или используемые для управления технологическими сетями связи и/или сетями связи специального назначения, а также на объекты, принадлежащие государственным органам.

Методические рекомендации направлены на детализацию и стандартизацию процедуры категорирования объектов критической информационной инфраструктуры, которая предусмотрена Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года N 187-ФЗ, а также содержат перечни:

– типовых процессов операторов связи, оказывающих услуги связи в сети связи общего пользования;

– типовых критических процессов операторов связи, оказывающих услуги связи в сети связи общего пользования;

– типовых информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, используемых операторами связи для оказания услуг связи в сети связи общего пользования;

– типовых объектов критической информационной инфраструктуры, принадлежащих операторам связи, оказывающим услуги связи в сети связи общего пользования.

Настоящий документ предназначен для членов комиссий по категорированию, создаваемых операторами связи, оказывающими услуги связи в сети связи общего пользования, и их работников, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов критической информационной инфраструктуры, а также для работников организаций, обладающих лицензией на деятельность по технической защите конфиденциальной информации, в случае их привлечения для проведения работ по обеспечению безопасности объектов критической информационной инфраструктуры, принадлежащих данным операторам связи.

Настоящий документ не содержит информацию ограниченного доступа.

Содержание

Термины и определения

В настоящем документе используются термины и соответствующие им определения, введенные действующими нормативными правовыми актами Российской Федерации, а также государственными стандартами и методическими документами.

Критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Объект критической информационной инфраструктуры – информационная система, информационно-телекоммуникационная сеть или автоматизированная система управления субъекта критической информационной инфраструктуры.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Автоматизированная система управления – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и/или производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами.

Сеть связи – технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи.

Сеть электросвязи – сеть связи, предназначенная для электросвязи (передача и прием сигналов, отображающих звуки, изображения, письменный текст, знаки или сообщения любого рода по электромагнитным системам).

Сеть связи общего пользования – сеть электросвязи, которая предназначена для возмездного оказания услуг электросвязи любому пользователю услугами связи на территории Российской Федерации и представляет собой комплекс взаимодействующих сетей электросвязи, в том числе сети связи для распространения программ телевизионного вещания и радиовещания.

Значимый объект критической информационной инфраструктуры – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

Безопасность критической информационной инфраструктуры – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

Субъект критической информационной инфраструктуры – государственный орган, государственное учреждение, российское юридическое лицо или индивидуальный предприниматель, которому на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российское юридическое лицо или индивидуальный предприниматель, которое обеспечивает взаимодействие указанных систем или сетей.

Компьютерная атака – целенаправленное воздействие программных и/или программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и/или прекращения их функционирования и/или создания угрозы безопасности обрабатываемой такими объектами информации.

Компьютерный инцидент – факт нарушения и/или прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и/или нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

Процесс – последовательность связанных действий или задач, необходимых для достижения определенного результата.

Услуга связи – деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений.

Продукт – материальная и/или нематериальная сущность, предлагаемая или предоставляемая оператором связи абоненту (клиенту).

Оператор связи – юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии.

Пользователь услугами связи – лицо, заказывающее и/или использующее услуги связи.

Абонент (клиент) – пользователь услугами связи, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации.

Муниципальное образование – городское или сельское поселение, муниципальный район, городской округ, городской округ с внутригородским делением, внутригородской район либо внутригородская территория города федерального значения.

Перечень принятых сокращений и обозначений

АРМ	–	Автоматизированное рабочее место
АСУ	–	Автоматизированная система управления
АСУМ	–	Автоматизированная система управления и мониторинга сетью
ИС	–	Информационная система
ИТКС	–	Информационно-телекоммуникационная сеть
КИИ	–	Критическая информационная инфраструктура
ЛВС	–	Локальная вычислительная сеть
ОКС N 7	–	Общеканальная сигнализация N 7
ПО	–	Программное обеспечение
СОРМ	–	Система технических средств для обеспечения функций оперативно-розыскных мероприятий
СрЗИ	–	Средство защиты информации
СУБД	–	Система управления базами данных
ФСБ России		Федеральная служба безопасности Российской Федерации
ФСТЭК России		Федеральная служба по техническому и экспортному контролю
AAA	–	Authentication, Authorization, Accounting
BSS	–	Business Support System
CDR	–	Call Detail Record
CRM	–	Customer Relationship Management
DCN	–	Data Communication Network
DNS	–	Domain Name System
DRA	–	Diameter Routing Agent
ERP	–	Enterprise Resource Planning
ESB	–	Enterprise Service Bus
eTOM	–	Enhanced Telecom Operations Map
GSM	–	Global System for Mobile Communications
HLR	–	Home Location Register
IVR	–	Interactive Voice Response
LTE	–	Long-Term Evolution
MAO	–	Maximum Allowable Outage
MVNO	–	Mobile Virtual Network Operator
NMS	–	Network Management System
NTP	–	Network Time Protocol
OSS	–	Operation Support System

RADIUS	–	Remote Authentication in Dial-In User Service
SMDR	–	Station Message Detail Record
SMS	–	Short Message Service
SMSC	–	Short Message Service Center
STP	–	Signalling Transfer Point
UMTS	–	Universal Mobile Telecommunications System
USSD	–	Unstructured Supplementary Service Data

1 Общие положения

Настоящий документ «Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи» (далее – методические рекомендации) разработан и утвержден в соответствии с подпунктом 7 пункта 2.3 Устава Общественно-государственного объединения «Ассоциация документальной электросвязи», утвержденного Министром Российской Федерации по связи и информатизации от 2 октября 2001 г.

Методические рекомендации детализируют и стандартизируют процедуру категорирования объектов критической информационной инфраструктуры (КИИ), принадлежащих на праве собственности, аренды или на ином законном основании государственным учреждениям, российским юридическим лицам и/или индивидуальным предпринимателям и используемых ими для осуществления видов деятельности в сфере связи, а именно возмездного оказания услуг электросвязи любому пользователю услуг связи на территории Российской Федерации на основании соответствующих лицензий.

Методические рекомендации предназначены для операторов связи, которые оказывают услуги связи в сети связи общего пользования согласно Федеральному закону от 7 июля 2003 года N 126-ФЗ «О связи» (далее – Федеральный закон N 126-ФЗ [1]), далее – операторы связи.

Методические рекомендации не предназначены для операторов выделенных сетей связи, технологических сетей связи и/или сетей связи специального назначения согласно Федеральному закону N 126-ФЗ [1].

Процедура категорирования объектов КИИ осуществляется на основании и в соответствии со статьей 7 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года N 187-ФЗ (далее – Федеральный закон N 187-ФЗ [2]), Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации и Перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 года N 127 (далее – Правила [3] и Перечень [3] соответственно).

Методические рекомендации применяются операторами связи:

– для определения процессов в рамках видов деятельности, осуществляемых операторами связи;

– выявления управленческих, технологических, производственных, финансово-экономических и/или иных процессов в рамках осуществления видов деятельности операторами связи, нарушение и/или прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения

обороны страны, безопасности государства и правопорядка (далее – критические процессы) из числа типовых процессов операторов связи;

– определения информационных систем (ИС), информационно-телекоммуникационных сетей (ИТКС) и автоматизированных систем управления (АСУ), которые обрабатывают информацию, необходимую для обеспечения критических процессов, и/или осуществляют управление, контроль или мониторинг критических процессов (далее совместно именуемых объекты КИИ), из числа типовых ИС, ИТКС и АСУ, принадлежащих операторам связи;

– формирования перечня объектов КИИ, подлежащих категорированию (далее – перечень объектов КИИ);

– оценки для каждого объекта КИИ в соответствии с Перечнем [3] масштаба возможных последствий в случае возникновения компьютерных инцидентов;

– присвоения каждому из объектов КИИ одной из категорий значимости либо принятия решения об отсутствии необходимости присвоения ему одной из категорий значимости;

– подготовки сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для направления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ.

По решению оператора связи представленный в методических рекомендациях перечень типовых объектов КИИ, принадлежащих операторам связи, может быть изменен, при этом:

– сокращение перечня типовых объектов КИИ осуществляется на основании отсутствия соответствующего типового объекта КИИ у оператора связи;

– расширение перечня типовых объектов КИИ осуществляется на основании самостоятельного решения оператора связи.

2 Отнесение оператора связи к субъектам критической информационной инфраструктуры, область применения методических рекомендаций

Отнесение любого государственного органа, государственного учреждения, российского юридического лица и/или индивидуального предпринимателя к субъектам КИИ осуществляется, исходя из его соответствия первым двум условиям (одновременно) или третьему условию:

1. Государственный орган, государственное учреждение, российское юридическое лицо и/или индивидуальный предприниматель осуществляет один или несколько из основных видов своей деятельности в одной или нескольких сферах (областях) деятельности, предусмотренных пунктом 8 статьи 2 Федерального закона N 187-ФЗ [2].

2. Государственному органу, государственному учреждению, российскому юридическому лицу и/или индивидуальному предпринимателю принадлежат на праве собственности, аренды или на ином законном основании любые ИС, ИТКС и АСУ.

3. Российское юридическое лицо и/или индивидуальный предприниматель обеспечивает взаимодействие ИС, ИТКС и АСУ, принадлежащих государственному ну, государственному учреждению, российскому юридическому лицу и/или индивидуальному предпринимателю, осуществляющему свою деятельность в одной или нескольких сферах (областях) деятельности, предусмотренных пунктом 8 статьи 2 Федерального закона N 187-ФЗ [2].

Если одно из первых двух условий и третье условие не выполняются, то государственный орган, государственное учреждение, российское юридическое лицо и/или индивидуальный предприниматель не является субъектом КИИ, если условия выполняются (одновременно первые два условия или третье условие), то является субъектом КИИ.

Область применения методических рекомендаций в отношении операторов связи как субъектов КИИ уточняется следующим образом:

– сферой деятельности, предусмотренной пунктом 8 статьи 2 Федерального закона N 187-ФЗ [2], является *связь*;

– в качестве субъектов КИИ рассматриваются государственные учреждения[1], российские юридические лица и/или индивидуальные предприниматели (не рассматриваются государственные органы), при этом не учитывается является ли оператор связи государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и/или стратегическим акционерным обществом, стратегическим предприятием;

[1] Казенное, бюджетное или автономное учреждение.

– рассматриваются объекты КИИ, используемые для оказания услуг связи в сети связи общего пользования на основании соответствующих лицензий (далее – услуги связи, перечень которых приведен ниже);

– для виртуальных операторов связи (Mobile Virtual Network Operator, MVNO) рассматриваются объекты КИИ, используемые ими на основании договора с HOST-оператором связи с учетом Требований [4];

– не рассматриваются объекты КИИ, используемые для оказания услуг операторами выделенных сетей связи, входящие в состав и/или используемые для управления технологическими сетями связи и/или сетями связи специального назначения (при этом перечень типовых процессов может быть использован ими для выявления критических процессов);

– не рассматриваются объекты КИИ, используемые операторами связи для осуществления видов деятельности в иных сферах, предусмотренных пунктом 8 статьи 2 Федерального закона N 187-ФЗ [2] (при этом перечень типовых процессов может быть использован ими для выявления критических процессов).

В методических рекомендациях на основании Перечня [5] определены следующие услуги связи, оказываемые операторами связи в сети связи общего пользования:

1. Услуги местной телефонной связи, за исключением услуг местной телефонной связи с использованием таксофонов и средств коллективного доступа.
2. Услуги междугородной и международной телефонной связи.
3. Услуги внутризоновой телефонной связи.
4. Услуги местной телефонной связи с использованием таксофонов.
5. Услуги местной телефонной связи с использованием средств коллективного доступа.
6. Услуги телеграфной связи.
7. Услуги связи персонального радиовызова.
8. Услуги подвижной радиосвязи в сети связи общего пользования.
9. Услуги подвижной радиотелефонной связи.
10. Услуги подвижной спутниковой радиосвязи.
11. Услуги связи по предоставлению каналов связи.
12. Услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации.
13. Услуги связи по передаче данных для целей передачи голосовой информации.
14. Телематические услуги связи.
15. Услуги связи для целей кабельного вещания.
16. Услуги связи для целей эфирного вещания.
17. Услуги связи для целей проводного радиовещания.

Оператор связи осуществляет определение оказываемых им услуг связи на основании:

– учредительных документов оператора связи (устава, положения, учредительного договора и т.п.);

– лицензий, выданных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций[2].

[2] Актуальный реестр лицензиатов в области связи доступен на веб-сайте: https://rkn.gov.ru/communication/register/license/.

3 Комиссия по категорированию объектов критической информационной инфраструктуры

Согласно пункту 2 Правил [3] категорирование объектов КИИ осуществляется оператором связи самостоятельно, для чего решением (приказом) руководителя оператора связи создается комиссия по категорированию объектов КИИ (далее – комиссия).

Форма приказа о создании комиссии приведена в приложении (см. Приложение А).

Создается одна комиссия в рамках одного оператора связи, для представительств и/или филиалов (в случае их наличия) отдельные комиссии не создаются.

В состав комиссии включаются:

– председатель комиссии: руководитель оператора связи (президент, генеральный директор или т.п.) или уполномоченное им лицо;

– члены комиссии:

  – работники оператора связи, являющиеся специалистами в области осуществляемых видов деятельности (специалисты в области телекоммуникаций (сетей электросвязи));

  – работники в области информационных технологий и связи (специалисты, обеспечивающие функционирование (администрирование) ИС, АСУ и/или ИТКС);

  – работники оператора связи, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов КИИ (специалисты, обеспечивающие функционирование (администрирование) систем и средств защиты информации);

  – работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций согласно Положению [6];

  – работники, ответственные за эксплуатацию основного технологического оборудования, технологическую (промышленную) безопасность;

  – работники подразделения по защите государственной тайны оператора связи (в случае, если с использованием объекта КИИ обрабатывают информацию, составляющую государственную тайну, и оператор связи обладает лицензией на проведение работ с использованием сведений, составляющих государственную тайну, выданной Федеральной службой безопасности Российской Федерации).

По решению оператора связи в состав комиссии могут быть включены другие работники оператора связи (например, экономисты, работники налоговой и юридической служб).

В состав комиссии по категорированию могут включаться представители Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по согласованию с данным министерством.

4 Определение процессов в рамках видов деятельности, осуществляемых оператором связи

Определение процессов в рамках видов деятельности, осуществляемых оператором связи (оказание услуг связи), проводится исходя из перечня типовых процессов операторов связи, оформленного в соответствии с национальным стандартом Российской Федерации «Расширенная схема деятельности организации связи (eTOM)» [7] (см. Таблица 1).

В рамках перечня типовых процессов операторов связи выделяются 3 главные области процессов [7]:

1. OPS – операционные (повседневные) процессы.
2. SIP – стратегические, инфраструктурные и продуктовые процессы.
3. EM – процессы управления организацией,

которые детализируются на нижележащих уровнях и представлены на рисунке и в таблице ниже (см. Рисунок 1, Таблица 1).

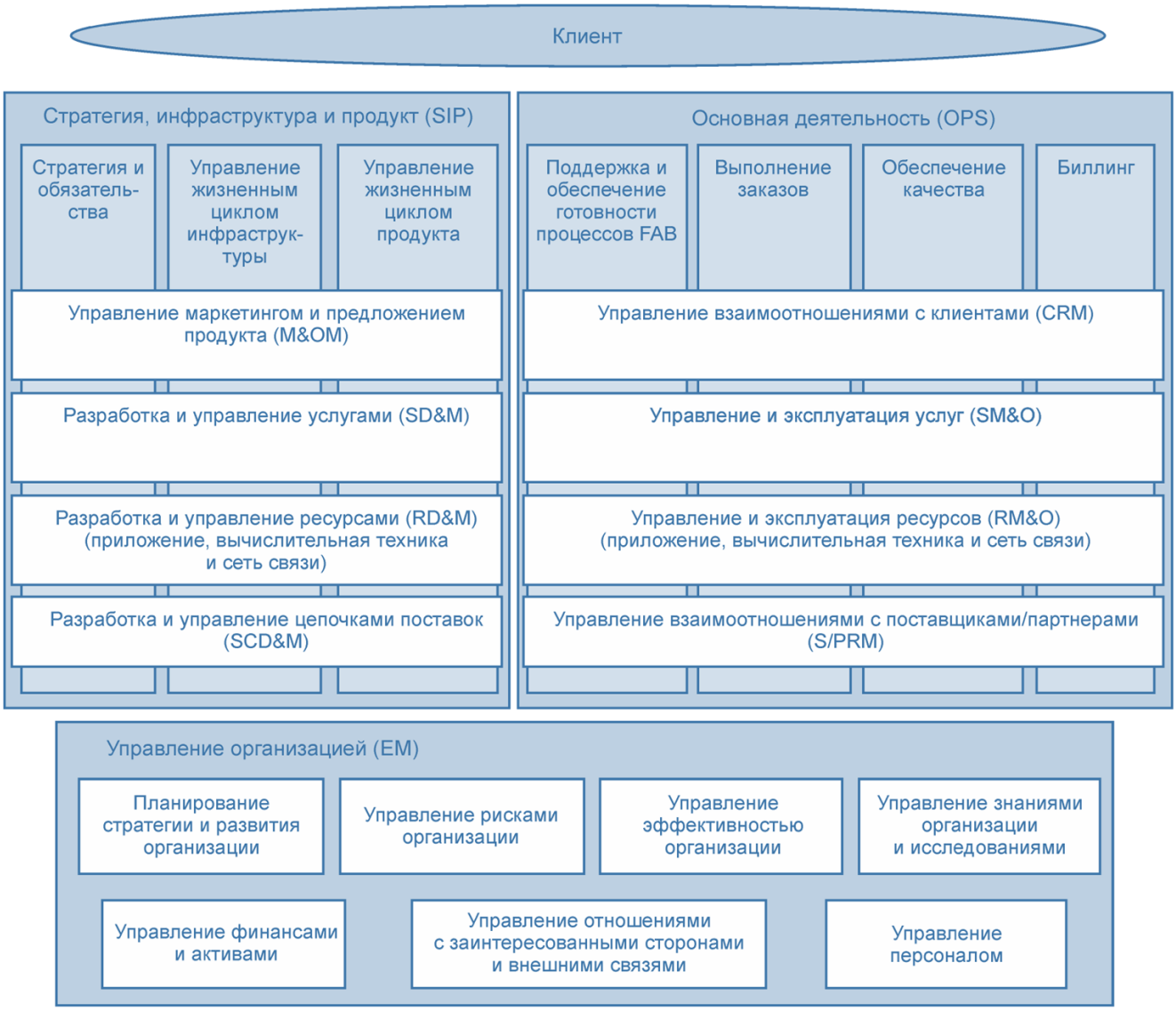

Рисунок 1 – Структура уровня 1 общей структуры процессов eTOM

Таблица 1 – Перечень типовых процессов операторов связи[3]

№	Наименование процесса	Назначение процесса
1.	**Операционные (повседневные) процессы (OPS)**	
1.1.	Управление взаимоотношениями с клиентами (CRM)	Процессы привлечения новых клиентов (взаимодействия с клиентами), расширения и сохранения отношений с существующими клиентами оператора связи (управление заказами, управление счетами с клиентами, маркетинг, продажи)
1.2.	Управление и эксплуатация услуг (SM&O)	Процессы предоставления, управления и поддержки функционирования услуг связи, используемых клиентами или предлагаемых им (достижение требуемого качества услуг, обеспечение удовлетворенности клиентов параметрами работы и стоимости услуг)
1.3.	Управление и эксплуатация ресурсов[4] (RM&O)	Процессы управления ресурсами, задействованными для предоставления и поддержки услуг связи, используемых клиентами или предлагаемых им (поддержка бесперебойного функционирования сетей электросвязи, обеспечение доступности ресурсов)
1.4.	Управление взаимоотношениями с поставщиками/партнерами (S/PRM)	Процессы приобретения продуктов и услуг связи у поставщиков и партнеров (управление заявками, управление счетами с поставщиками/партнерами, управление качеством продуктов поставщиков/партнеров)
2.	**Стратегические, инфраструктурные и продуктовые процессы (SIP)**	
2.1.	Управление маркетингом и предложением продукта (M&OM)	Процессы, обеспечивающие выполнение обязательств оператора связи по получению доходов, выпуску продукции, прибылям и убыткам (разработка стратегий и новых продуктов, формирование и управление сбытом, реализация стратегий маркетинга)
2.2.	Разработка и управление услугами (SD&M)	Процессы планирования, разработки и подготовки услуг связи для их последующего использования процессами главной области OPS (формирование стратегий развития услуг оператора связи, формирование инфраструктуры услуг, разработка услуг и отзыв с рынка)
2.3.	Разработка и управление ресурсами (RD&M)	Процессы планирования, разработки и подготовки ресурсов, необходимых процессам главной области OPS для предоставления клиентам услуг и продуктов (формирование стратегий развития ресурсов оператора связи, развитие инфраструктуры ресурсов, разработка ресурсов и вывод из эксплуатации)

[3] 1 уровень общей структуры процессов eTOM, горизонтальные группы процессов [7].
[4] К ресурсам относятся приложения (программное средства), вычислительная техника (программно-аппаратные средства) и сети электросвязи.

№	Наименование процесса	Назначение процесса
2.4.	Разработка и управление цепочками поставок (SCD&M)	Процессы взаимодействия с поставщиками/партнерами, участвующими в цепочках поставок (формирование стратегии и политики оператора связи применительно к цепочкам поставок, формирование цепочек поставок, развитие цепочек поставок и управления изменениями)
3.	**Процессы управления организацией (EM)**	
3.1.	Планирование стратегии и развития организации (S&EP)	Процессы разработки стратегии и планов развития оператора связи (определение направлений развития бизнеса, выбор рынков, определение требований к финансированию)
3.2.	Управление рисками организации (ERM)	Процессы выявления рисков и угроз доходам или репутации оператора связи, выполнения необходимых управляющих действий, включая обеспечение непрерывности бизнеса, управление безопасностью и борьбу с мошенничеством
3.3.	Управление эффективностью организации (EEM)	Процессы совершенствования процессов, обеспечения эффективности процессов управления программами развития и проектами, качеством продукции и производительностью оператора связи
3.4.	Управление знаниями организации и исследованиями (K&RM)	Процесс управления знаниями оператора связи, исследованиями технологий и оценками целесообразности приобретения новых технологий
3.5.	Управление финансами и активами (F&AM)	Процессы контроля движения активов оператора связи и управления бухгалтерским балансом оператора связи
3.6.	Управление отношениями с заинтересованными сторонами и внешними связями (S&ERM)	Процессы управления отношениями с акционерами, внешние связи, трудовые отношения и связи с общественностью
3.7.	Управление персоналом (HRM)	Управление трудовыми отношениями в рамках оператора связи с учетом Трудового кодекса Российской Федерации [8]

5 Выявление критических процессов в рамках видов деятельности, осуществляемых оператором связи

5.1 Виды негативных последствий

Выявление критических процессов осуществляется оператором связи на базе перечня типовых процессов операторов связи (см. Таблица 1), исходя из того, что нарушение и/или прекращение типового процесса может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

Виды негативных последствий и связанные с ними показатели критериев значимости объектов КИИ, установленные Перечнем [3], представлены на рисунке ниже (см. Рисунок 2).

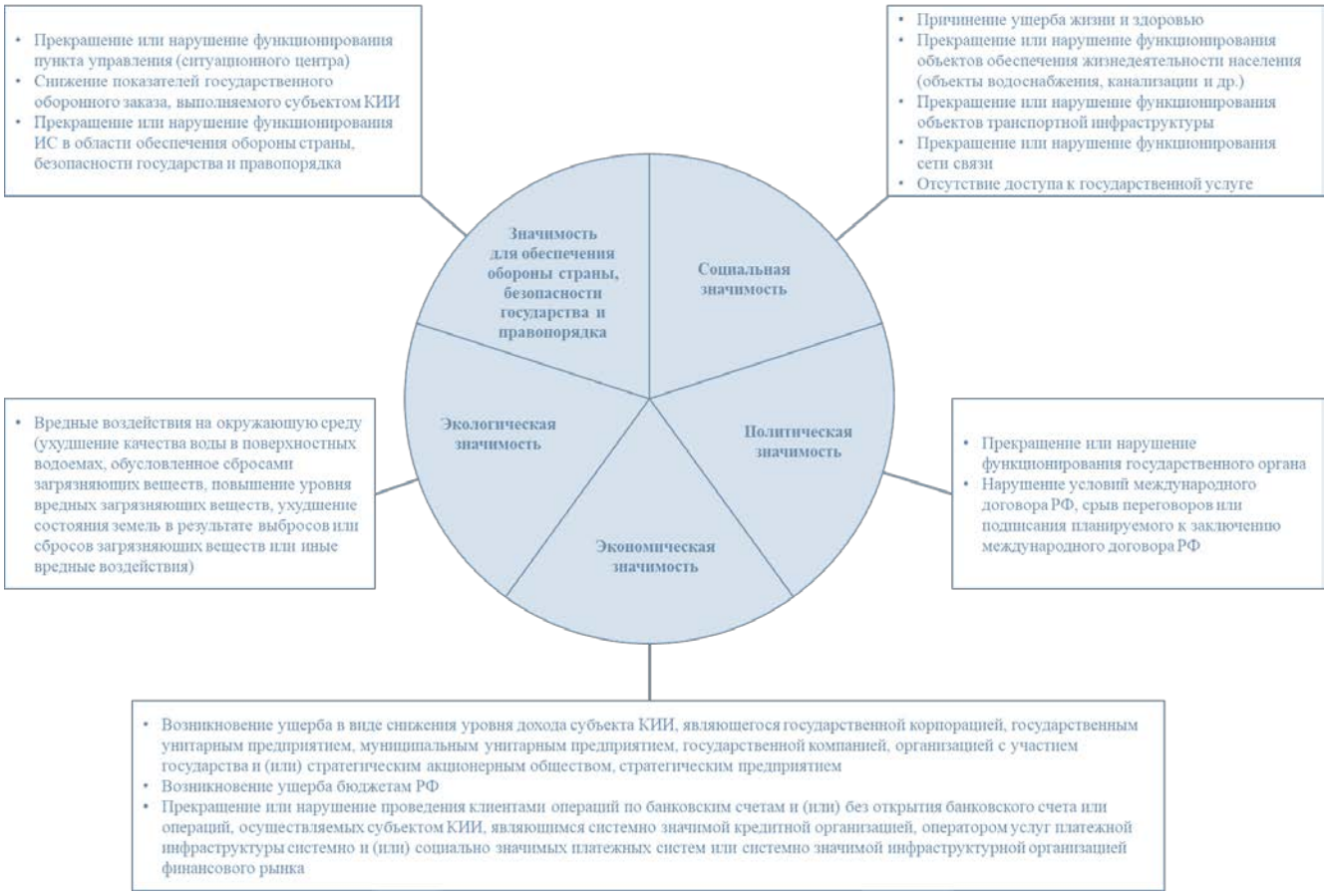

Рисунок 2 – Виды негативных последствий

Принимая во внимание, что в методических рекомендациях рассматриваются операторы связи, осуществляющие виды деятельности в сфере *связи*, а именно *возмездно оказывающие услуги электросвязи* любому пользователю услуг связи на территории Российской Федерации, в том числе *государственным органам власти*, то далее рассматриваются следующие виды негативных последствий:

1. «Прекращение или нарушение функционирования сети связи», которое оценивается:

– по территории, на которой возможно прекращение или нарушение функционирования сети связи;

– количеству людей, для которых могут быть недоступны услуги связи.

2. «Возникновение ущерба бюджетам Российской Федерации», который оценивается в снижении доходов (процентов прогнозируемого годового дохода бюджета):

– федерального бюджета;

– бюджета субъекта Российской Федерации;

– бюджетов государственных внебюджетных фондов.

3. «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)».

Помимо обозначенных выше видов негативных последствий по решению оператора связи могут быть дополнительно рассмотрены и другие виды негативных последствий и связанные с ними показатели критериев значимости объектов КИИ, приведенные в Перечне [3].

При этом с учетом положений Федерального закона N 187-ФЗ [2] в качестве причины возникновения негативных последствий рассматривается только компьютерные инциденты вследствие компьютерных атак, т.е. не рассматриваются случаи, когда:

– оператор связи прекращает и/или ограничивает оказание услуг электросвязи на основании Правил оказания услуг связи [9-11] или договора возмездного оказания услуг между абонентом и оператором связи;

– прекращение и/или нарушение оказания услуг электросвязи вызвано техногенной аварией, природным явлением и/или стихийным бедствием;

– прекращение и/или нарушение оказания услуг электросвязи вызвано непреднамеренными действиями оператора связи, пользователей услугами связи или третьих лиц (обрыв линий связи, создание аварийных ситуаций в отношении средств связи и т.п.).

5.2 Прекращение или нарушение функционирования сети связи

Под прекращением или нарушением функционирования сети связи с учетом положений проекта Концепции управления качеством связи в Российской Федерации [12] в методических рекомендациях рассматривается ситуация недоступности услуги связи, т.е. невозможность обеспечить (установить) соединение для передачи и/или приема сообщений электросвязи по указанному при запросе адресу (уникальному коду идентификации) с учетом условий договора возмездного оказания услуг между абонентом и оператором связи. Данная невозможность обеспечить (установить) соединение оценивается:

– по территории, на которой невозможно обеспечить (установить) соединение;

– количеству людей (абонентов оператора связи), которые не могут установить соединение.

5.3 Возникновение ущерба бюджетам Российской Федерации

Под возникновением ущерба федеральному бюджету Российской Федерации с учетом положений закона или законопроекта о федеральном бюджете на соответствующий год[5], а также Налогового кодекса Российской Федерации [14] в методических рекомендациях рассматривается ситуация неуплаты (сокращения уплаты) федеральных налогов и сборов, а именно[6]:

- налога на добавленную стоимость;
- налога на прибыль организации.

Под возникновением ущерба бюджету субъекта Российской Федерации с учетом положений Налогового кодекса Российской Федерации [14] в методических рекомендациях рассматривается ситуация неуплаты (сокращения уплаты) региональных налогов, а именно налога на прибыль организации[7].

Под возникновением ущерба бюджету государственных внебюджетных фондов с учетом положений проекта основных направлений бюджетной, налоговой и таможенно-тарифной политики на 2019 год и на плановый период 2020 и 2021 годов [15] в методических рекомендациях рассматривается ситуация неуплаты (сокращения уплаты) страховых взносов, а именно:

- взносов на обязательное пенсионное страхование;
- взносов на обязательное социальное страхование;
- взносов на обязательное медицинское страхование.

Принимая во внимание, что в методических рекомендациях рассматривается цепочка событий, вызванная компьютерной атакой и приводящая к негативным экономическим последствиям (см. Рисунок 3), то в качестве конечного ущерба бюджетам Российской Федерации далее рассматриваются только следующие ситуации неуплаты (сокращения уплаты) налогов:

- федеральных налогов: налога на прибыль организации;
- региональных налогов: налога на прибыль организации.

---

[5] Для 2019 года: Федеральный закон о федеральном бюджете на 2019 год [13].

[6] Для операторов связи не рассматриваются иные источники доходов федерального бюджета, не связанные с осуществлением видов деятельности в сфере связи (акцизы, налоги на добычу полезных ископаемых, водный налог, сборы за пользование объектами животного мира и за пользование объектами водных биологических ресурсов, государственные пошлины).

[7] Для операторов связи не рассматриваются иные источники доходов бюджета субъекта Российской Федерации, не связанные с осуществлением видов деятельности в сфере связи (налог на имущество организации, земельный налог, налог на игровой бизнес, транспортный налог).

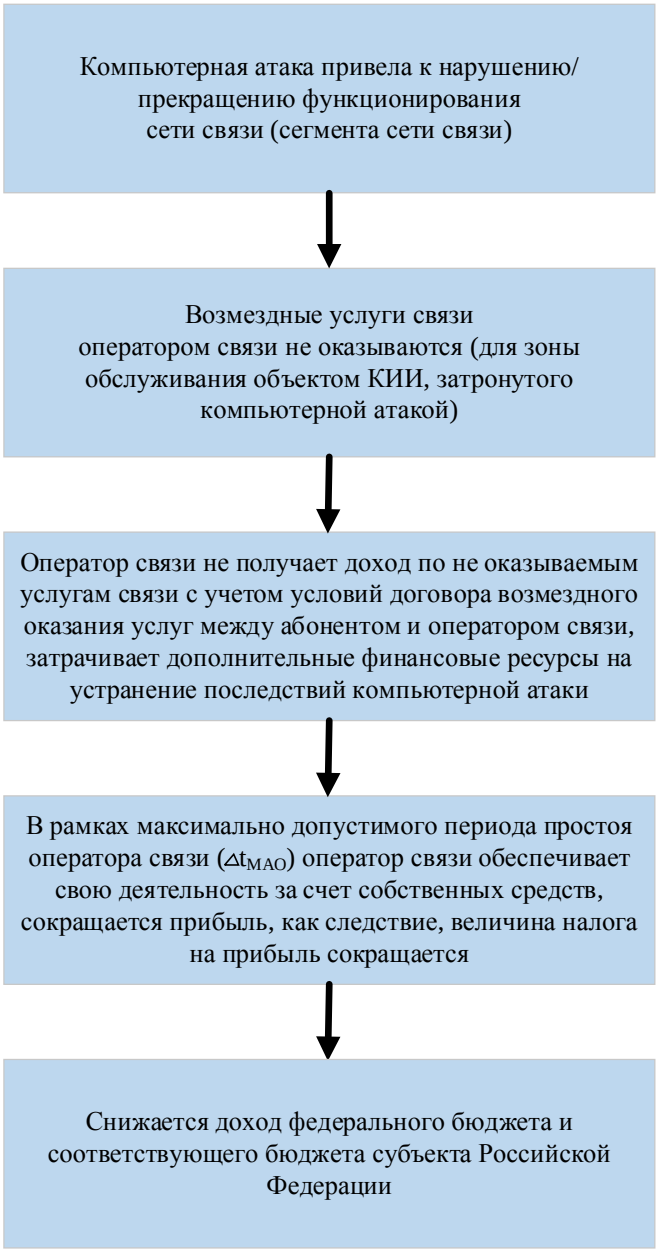

Рисунок 3 – Цепочка событий, вызванная компьютерной атакой и приводящая к негативным экономическим последствиям

5.4 Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)

Под прекращением или нарушением функционирования государственного органа в части невыполнения возложенной на него функции (полномочия) с учетом положений федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [16] в методических рекомендациях рассматривается ситуация невозможности для государственного органа реализации возложенных на него функций (полномочий), закрепленных в соответствующих нормативно-правовых актах Российской Федерации, в результате недоступности услуги связи, приобретенной им в рамках государ-

ственного контракта для выполнения возложенной на него функции (полномочия), с учетом условий данного контракта[8].

В обязательном порядке оператором связи рассматриваются следующие услуги связи, оказываемые им государственному органу в сети связи общего пользования с учетом условий государственного контракта:

- услуги местной телефонной связи;
- услуги междугородной и международной телефонной связи;
- услуги внутризоновой телефонной связи;
- услуги связи по предоставлению каналов связи;
- услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации;
- услуги связи по передаче данных для целей передачи голосовой информации.

Не рассматриваются ситуации (случаи) недоступности следующих услуг связи, оказываемых операторами связи государственным органам в сети связи общего пользования в рамках государственных контрактов:

- услуги подвижной радиосвязи в сети связи общего пользования;
- услуги подвижной радиотелефонной связи;
- услуги, оказываемые с использованием радиоэлектронных средств стандартов GSM, UMTS, LTE и их последующих модификаций,

а также ситуации, когда с использованием указанных услуг государственные органы получают доступ к другим услугам связи (например, к услугам междугородной и международной телефонной связи, услугам по передаче данных и др.).

Не рассматриваются ситуации (случаи) неработоспособности выделенных сетей связи, технологических сетей связи и/или сетей связи специального назначения, а также оборудования, принадлежащего государственным органам.

Данный вид негативных последствий может возникнуть только в случае наличия у оператора связи соответствующего действующего государственного контракта с органом государственной власти, приведенным в приложении (см. Приложение Б), с учетом исключений, приведенных выше.

Данный вид негативных последствий оценивается по уровню органа государственной власти, с которым заключен соответствующий государственный контракт:

- орган государственной власти субъекта Российской Федерации или города федерального значения;

[8] Условия государственного контракта определяют штатные параметры оказания услуги связи.

– федеральный орган государственной власти;

– Администрация Президента Российской Федерации, Правительство Российской Федерации, Федеральное Собрание Российской Федерации, Совет Безопасности Российской Федерации, Верховный Суд Российской Федерации, Конституционный Суд Российской Федерации.

5.5 Перечень типовых критических процессов оператора связи

Для указанных видов негативных последствий в методических рекомендациях выделены типовые критические процессы операторов связи с учетом положений национальных стандартов Российской Федерации «Расширенная схема деятельности организации связи (eTOM)» [7, 17, 18] (см. Таблица 2).

Таблица 2 – Перечень типовых критических процессов оператора связи

№	Наименование критического процесса	Назначение критического процесса	Обоснование критичности процесса
Область «Операционные (повседневные) процессы (OPS)»			
1.	Управление и эксплуатация услуг (SM&O)	Процессы предоставления, управления и поддержки функционирования услуг связи, используемых клиентами или предлагаемых им (достижение требуемого качества услуг, обеспечение удовлетворенности клиентов параметрами работы и стоимости услуг)	Нарушение и/или прекращение данного процесса может привести к прекращению и/или ограничению оказания услуг связи, т.е. негативному последствию «Прекращение или нарушение функционирования сети связи», а также «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» (в случае наличия соответствующего государственного контракта). Невозможность оказания услуг связи может привести к сокращению прибыли оператора связи и, как следствие, может привести к сокращению/неуплате налогов (взносов), т.е. негативному последствию «Возникновение ущерба бюджетам Российской Федерации»

№	Наименование критического процесса	Назначение критического процесса	Обоснование критичности процесса
Область «Операционные (повседневные) процессы (OPS)»			
2.	Управление и эксплуатация ресурсов (RM&O)	Процессы управления ресурсами, задействованными для предоставления и поддержки услуг связи, используемых клиентами или предлагаемых им (поддержка бесперебойного функционирования сетей электросвязи, обеспечение доступности ресурсов)	Нарушение и/или прекращение данного процесса может привести к прекращению и/или ограничению работоспособности ресурсов и, как следствие, может привести к прекращению и/или ограничению оказания услуг связи, т.е. негативному последствию «Прекращение или нарушение функционирования сети связи», а также «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» (в случае наличия соответствующего государственного контракта). Невозможность оказания услуг связи может привести к сокращению прибыли оператора связи и, как следствие, может привести к сокращению/неуплате налогов (взносов), т.е. негативному последствию «Возникновение ущерба бюджетам Российской Федерации»

6 Определение объектов критической информационной инфраструктуры

Определение объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и/или осуществляют управление, контроль или мониторинг критических процессов, осуществляется оператором связи на базе перечня типовых ИС, ИТКС и АСУ операторов связи, приведенного в приложении (см. Приложение В), исходя из перечня типовых критических процессов операторов связи (см. Таблица 2).

Группировка типовых ИС, ИТКС и АСУ операторов связи, а также сетей электросвязи представлена на рисунке ниже (см. Рисунок 4).

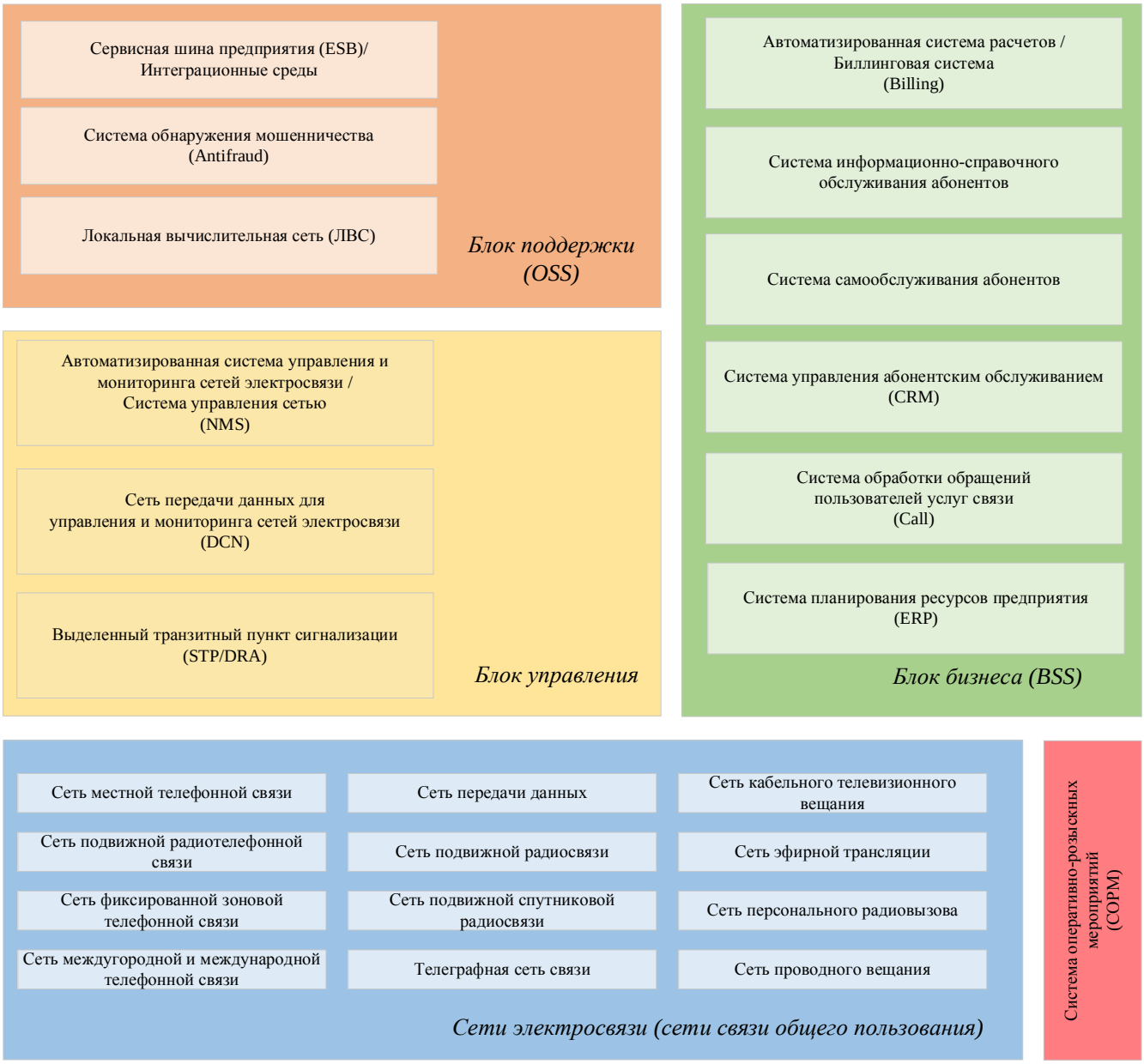

Рисунок 4 – Группировка типовых ИС, ИТКС, АСУ, сетей электросвязи операторов связи

Принимая во внимание, что сеть электросвязи[9] не является ИТКС, а также с учетом определения термина КИИ, введенного Федеральным законом N 187-ФЗ [2], сети электросвязи (т.е. средства и линии связи, предназначенные для электросвязи) не являются объектами КИИ и в составе типовых ИС, ИТКС и АСУ операторов связи не рассматриваются.

Требования к функционированию единой сети электросвязи Российской Федерации (неотъемлемой частью которой выступает сеть связи общего пользования согласно Федеральному закону N 126-ФЗ [1]), связанные с обеспечением целостности, устойчивости функционирования указанной сети электросвязи и ее безопасности, отношения, связанные с обеспечением целостности единой сети связи Российской Федерации и использованием радиочастотного спектра, соответственно устанавливаются и регулируются законодательством Российской Федерации в области связи.

С использованием перечня типовых ИС, ИТКС и АСУ, принадлежащих операторам связи (см. Приложение В), исходя из их назначения, в методических рекомендациях определены типовые объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения типовых критических процессов операторов связи (см. Таблица 2), и/или осуществляют управление, контроль или мониторинг данных процессов (см. Таблица 3, Таблица 4).

Описание назначения и логические схемы типовых объектов КИИ, принадлежащих операторам связи, приведены в приложениях (Приложение В, Приложение Г).

[9] Понятие сети электросвязи введено в Федеральном законе N 126-ФЗ [1] и национальном стандарте Российской Федерации «Связь федеральная. Термины и определения» [19].

Таблица 3 – Типовые ИС, ИТКС и АСУ операторов связи, задействованные в реализации типовых критических процессов

№	Наименование типового критического процесса	Наименование типового объекта КИИ			
		Обработка[10]	**Управление**[11]	**Контроль**[12]	**Мониторинг**[13]
1.	Управление и эксплуатация услуг (SM&O)	Выделенные транзитные пункты сигнализации	Автоматизированные системы расчетов[14]. Системы самообслуживания абонентов. Выделенные транзитные пункты сигнализации. Автоматизированные системы управления и мониторинга сетей электросвязи	Автоматизированные системы расчетов. Автоматизированные системы управления и мониторинга сетей электросвязи	Автоматизированные системы расчетов. Автоматизированные системы управления и мониторинга сетей электросвязи
2.	Управление и эксплуатация ресурсов (RM&O)	Выделенные сети передачи данных для управления и мониторинга сетей электросвязи	Автоматизированные системы управления и мониторинга сетей электросвязи	Автоматизированные системы управления и мониторинга сетей электросвязи	Автоматизированные системы управления и мониторинга сетей электросвязи

[10] Обработка – систематическое выполнение операций над данными, необходимыми для обеспечения критического процесса.
[11] Управление – поддержание критического процесса в рабочем состоянии в рамках заданных значений характеристик критического процесса.
[12] Контроль – сравнение (сопоставление) фактических (текущих) значений характеристик критического процесса с заданными значениями этих характеристик.
[13] Мониторинг – постоянное (регулярное) наблюдение за значениями характеристик критического процесса.
[14] Для схемы расчетов «prepaid» (оказание услуги связи осуществляется на базе решения от данной ИС).

Далее в методических рекомендациях детализируются и стандартизируются процедуры категорирования, предусмотренные Федеральным законом N 187-ФЗ [2], только в отношении типовых объектов КИИ, принадлежащих операторам связи, указанных в таблице ниже (см. Таблица 4).

Таблица 4 – Перечень типовых объектов КИИ, принадлежащих операторам связи

№	Наименование типового объекта КИИ	Обоснование выбора
1.	Автоматизированные системы расчетов[15] / Биллинговые системы (Billing)	Обеспечивают автоматизацию учета оказываемых услуг связи (мониторинг и контроль критического процесса). Приостанавливают оказание услуг связи (управление критическим процессом, если позволяет функционал)
2.	Системы самообслуживания абонентов[16]	Обеспечивают автоматизацию управления (подключения/отключения) услуг связи (управление критическим процессом)
3.	Автоматизированные системы управления и мониторинга сетей электросвязи[17] / Системы управления сетью (Network Management Systems (NMS))	Обеспечивают автоматизацию управления услугами связи и ресурсами (управление и/или мониторинг и контроль критического процесса)
4.	Выделенные транзитные пункты сигнализации[18] (Signalling Transfer Point (STP) / Diameter Routing Agent (DRA))	Обеспечивают автоматизацию управления сетью сигнализации и обработки сообщений сигнализации (управление критическим процессом, обработка (передача) информации)
5.	Выделенные сети передачи данных[19] для управления и мониторинга сетей электросвязи (Data Communication Network (DCN))	Обеспечивают передачу информации между автоматизированными системами управления и мониторинга сетей связи и объектами управления (обработка (передача) информации)

[15] Понятие «Автоматизированные системы расчетов» введено согласно Правилам применения автоматизированных систем расчетов [20].

[16] Понятие «Система самообслуживания» введено согласно Правилам оказания услуг связи [9, 10].

[17] Понятие «Автоматизированные системы управления и мониторинга сетями электросвязи» введено согласно Перечню средств связи, подлежащих обязательной сертификации [21].

[18] Понятие «Выделенный транзитный пункт сигнализации» введено согласно Правилам применения оборудования автоматизированных систем управления и мониторинга сетей электросвязи [22].

[19] Понятие «Выделенные сети передачи данных» введено согласно документу «Построение систем управления сетями связи операторов взаимоувязанной сети связи Российской Федерации» [23].

Данные сети используют специально выделенные для них средства связи.

Если данная сеть построена на средствах связи, входящих в состав сетей электросвязи оператора связи, в т.ч. транспортной сети, то она не рассматривается как объект КИИ.

7 Формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию

Формирование перечня объектов КИИ осуществляется оператором связи с использованием перечня типовых объектов КИИ, принадлежащих операторам связи (см. Таблица 3), исходя из реального состава ИС, АСУ и ИТКС, принадлежащих оператору связи на праве собственности, аренды или на ином законном основании.

Оформление перечня объектов КИИ осуществляется в соответствии с Рекомендуемой ФСТЭК России формой [24] с учетом рекомендаций, приведенных в таблице ниже (см. Таблица 5).

Сформированный перечень объектов КИИ утверждается руководителем оператора связи (президентом, генеральным директором или т.п.) или уполномоченным им лицом.

Отправка сформированного и утвержденного перечня объектов КИИ осуществляется[20] в течение пяти рабочих дней с даты его утверждения в адрес федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры (экспедиция центрального аппарата ФСТЭК России): Москва, ул. Старая
Басманная, д. 17[21], на бумажном носителе и на электронном носителе информации (компакт-диск, USB-накопитель или т.п.) в DOC(X)/XLS(S)-формате.

Таблица 5 – Рекомендации по заполнению формы перечня объектов КИИ оператора связи, подлежащих категорированию

№	Наименование объекта	Тип объекта	Сфера (область) деятельности, в которой функционирует объект	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя[22], его телефон, адрес электронной почты (при наличии)
1.	Автоматизированная система расчетов «*Наименование*»	Информационная система	Связь	до *ДД.ММ.ГГГГ*[23]	*Должность, фамилия, имя, отчество, номер телефон, адрес электронной почты*

[20] Если у оператора связи нет на праве собственности, аренды или ином законном основании ни одного из указанных типовых объектов КИИ и каких-либо других объектов КИИ, то не осуществляется отправка пустого перечня объектов КИИ.
[21] Актуальный адрес и режим работы экспедиция центрального аппарата ФСТЭК России доступны на веб-сайте: https://fstec.ru/kontakty.
[22] Указывается представитель оператора связи, который может предоставить дополнительные данные по конкретному объекту КИИ (назначение, архитектура, состав и т.п.) в случае обращения представителя ФСТЭК России.
[23] Указывается дата в интервале до 1 года (365 дней) с даты утверждения оператором связи перечня объектов КИИ.

№	Наименование объекта	Тип объекта	Сфера (область) деятельности, в которой функционирует объект	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя[22], его телефон, адрес электронной почты (при наличии)
2.	Система самообслуживания абонентов «*Наименование*»	Информационная система	Связь	до *ДД.ММ.ГГГГ*	*Должность, фамилия, имя, отчество, номер телефон, адрес электронной почты*
3.	Автоматизированная система управления и мониторинга сетей электросвязи «*Наименование*»	Автоматизированная система управления	Связь	до *ДД.ММ.ГГГГ*	*Должность, фамилия, имя, отчество, номер телефон, адрес электронной почты*
4.	Выделенный транзитный пункт сигнализации «*Наименование № Х*»	Автоматизированная система управления	Связь	до *ДД.ММ.ГГГГ*	*Должность, фамилия, имя, отчество, номер телефон, адрес электронной почты*
5.	Выделенная сеть передачи данных для управления и мониторинга сетей электросвязи «*Наименование № Х*»	Информационно-телекоммуникационная сеть	Связь	до *ДД.ММ.ГГГГ*	*Должность, фамилия, имя, отчество, номер телефон, адрес электронной почты*

Дополнительные рекомендации по заполнению формы перечня объектов КИИ оператора связи, подлежащих категорированию:

1. Если у оператора связи нет на праве собственности, аренды или ином законном основании соответствующего типового объекта КИИ (например, нет системы самообслуживания абонентов), то данные по этому типовому объекту КИИ не указываются (строка в перечне объектов КИИ удаляется).

2. Если у оператора связи несколько однотипных объектов КИИ (например, несколько автоматизированных систем расчетов), то указывается каждый объект КИИ в отдельной строке с соответствующим наименованием (строки в перечне объектов КИИ добавляются).

3. Если у оператора связи несколько однотипных объектов КИИ с одинаковым наименованием (например, несколько однотипных выделенных транзитных пунктов сигнализации с

одинаковым наименованием), то указывается каждый объект КИИ в отдельной строке с соответствующим наименованием и порядковым/инвентарным номером (строки в перечне объектов КИИ добавляются).

4. В качестве наименования объекта КИИ указывается наименование, приведенное в одном из следующих локальных актов, оформленных оператором связи, или документов:

– акт ввода в эксплуатацию, оформленный оператором связи согласно Требованиям [25];

– паспорт организации связи по информационной безопасности, оформленный оператором связи согласно национальному стандарту [26];

– сертификат соответствия в системе сертификации в области связи[24] (применимо только для сертифицированного средства);

– эксплуатационная документации от производителя или наименование производителя (например, Автоматизированная система расчетов от «*Наименование производителя*»).

Данные наименования используются с целью однозначной идентификации объекта КИИ в инфраструктуре оператора связи (при необходимости вводятся порядковые/инвентарные номера или другие идентификаторы).

5. Для типового объекта КИИ «Выделенная сеть передачи данных для управления и мониторинга сетей электросвязи» в качестве наименования указывается сокращенное фирменное наименование оператора связи на русском языке и порядковый/инвентарный номер сети, если их несколько (например, Выделенная сеть передачи данных для управления и мониторинга сетей электросвязи «*Наименование оператора связи*» №1).

[24] Реестр зарегистрированных сертификатов соответствия на средства связи доступен на веб-сайте: https://www.rossvyaz.ru/activity/correlation/certification/registerCertificate/.

8 Оценка масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры

Оценка масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ, принадлежащих оператору связи, осуществляется оператором связи, исходя:

– из масштабов самого объекта КИИ (количества абонентов и зоны обслуживания);

– наличия возможности реализации угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ, последствиями которых будут нарушение и/или прекращение функционирования сети связи;

– размера налогов, сборов и взносов оператора связи в соответствующие бюджеты Российской Федерации (сумма за отчетный (годовой) период), а также максимально допустимого периода простоя оператора связи (неоказания оператором связи услуг связи)[25];

– наличия действующего соответствующего государственного контракта на оказание услуг связи органу государственной власти (с учетом исключений, указанных в п 5.4).

В рамках оценки масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ, принадлежащих оператору связи, оператором связи для каждого конкретного объекта КИИ осуществляются действия в следующем порядке:

1. Оценивается масштаб конкретного объекта КИИ, исходя из территории, которую обслуживает данный объект КИИ (зона обслуживания с привязкой к субъектам Российской Федерации), и количества обслуживаемых абонентов, с учетом типа объекта КИИ согласно таблице ниже (см. Таблица 6).

[25] Период времени, по истечении которого существует угроза окончательной утраты жизнеспособности оператора связи, в том случае, если оказание услуг связи не будет возобновлено.

Таблица 6 – Параметры оценки масштабов типовых объектов КИИ, принадлежащих операторам связи

№	Наименование типового объекта КИИ	Название параметра оценки масштаба типового объекта КИИ	
		Количество абонентов[26]	**Зона обслуживания**[27]
1.	Автоматизированная система расчетов	Количество абонентов, обслуживаемых данной системой, или емкость сети, указанная в сертификате соответствия на данную систему[28]	Территория, с которой средства связи отправляют CDR/SMDR-файлы в данную систему
2.	Система самообслуживания абонентов	Количество абонентов, обслуживаемых данной системой (количество активных в течение года учетных записей пользователей в данной системе)	Территория, для которой осуществляется управление оказываемыми услугами связи с использованием данной системы
3.	Автоматизированная система управления и мониторинга сетей электросвязи	Количество абонентов сети электросвязи, управляемой данной системой (абонентская емкость сети электросвязи)	Территория, обслуживаемая средствами связи, которыми управляет данная система
4.	Выделенный транзитный пункт сигнализации	Количество абонентов сети электросвязи (зоны в сети электросвязи), в которой размещен данный пункт сигнализации (абонентская емкость сети/зоны в сети электросвязи)	Территория, которую обслуживает данный пункт сигнализации
5.	Выделенная сеть передачи данных для управления и мониторинга сетей электросвязи	Суммарное количество абонентов, указанное для всех автоматизированных систем управления и мониторинга сетей электросвязи, использующих данную выделенную сеть для управления и мониторинга	Территория, обслуживаемая средствами связи, которыми управляют с использованием данной выделенной сети

2. Оценивается наличие возможности реализации угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ, послед-

[26] Общее количество абонентов определяется на основании количества заключенных с физическими (юридическими) лицами договоров на момент проведения категорирования объектов КИИ, принадлежащих оператору связи.
[27] На практике зона обслуживания выходит за территорию одного муниципального образования или одной внутригородской территории города федерального значения.
[28] Указывается доступный оператору связи параметр.

ствиями которых будут нарушение и/или прекращение функционирования сети связи, с использованием модели нарушителя и перечня основных угроз безопасности информации (см. Приложение Д, Приложение Е).

В рамках оценки возможности реализации угроз безопасности информации оператором связи учитывается, что в качестве мер противодействия угрозам безопасности информации рассматриваются только организационные, механические и/или аналоговые меры, т.е. меры которые не могут быть подвержены компьютерным атакам (например, физические и механические меры ограничения непосредственного доступа к объектам КИИ, аналоговые каналы управления, механические переключатели и др.).

Если для конкретного объекта КИИ существует возможность реализации угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ, последствиями которых будут нарушение и/или прекращение функционирования сети связи, то конкретному объекту КИИ потенциально может быть присвоена одна из категорий значимости (требуется оценка масштаб возможных негативных последствий), если нет, то отсутствует необходимость присвоения конкретному объекту КИИ одной из категорий значимости.

Если существует возможность реализации угроз безопасности информации, которые приводят только к нарушению и/или прекращению функционирования объекта КИИ, но не влекут за собой нарушение и/или прекращение функционирования сети связи, то отсутствует необходимость присвоения конкретному объекту КИИ одной из категорий значимости.

3. Оценивается масштаб возможных негативных последствий, исходя из того, что рассматривается самый худший сценарий реализации угрозы безопасности информации, т.е. масштаб ущерба от компьютерного инцидента (нарушения и/или прекращения функционирования сети связи) равен масштабу объекта КИИ, а также принимается во внимание, что оказание услуг электросвязи не может быть реализовано альтернативными (нетехнологическими) решениями.

3.1. Сопоставляется масштаб объекта КИИ со значениями (диапазонами значений), приведенными в таблице ниже для показателя «Прекращение или нарушение функционирования сети связи» (см.

3.2. Таблица 7).

Таблица 7 – Значения показателей «Прекращение или нарушение функционирования сети связи»

№	Наименование показателя	III категория	II категория	I категория
Прекращение или нарушение функционирования сети связи, оцениваемые				
1.	а) на территории, на которой возможно прекращение или нарушение функционирования сети связи	Вся территория одного муниципального образования или одной внутригородской территории города федерального значения	Выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	Выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
2.	б) по количеству людей, для которых могут быть недоступны услуги связи (человек)	Более или равно 50 000, но менее 1 000 000	Более или равно 1 000 000, но менее 5 000 000	Более или равно 5 000 000

3.3. Для сопоставления со значениями, приведенными в таблице ниже для показателя «Возникновение ущерба бюджетам Российской Федерации» (см. Таблица 8), рассчитываются значения потенциально возможного ущерба бюджетам Российской Федерации.

Определяется актуальный годовой размер выплачиваемых оператором связи налогов в бюджеты Российской Федерации, исходя из данных, предоставляемых оператором связи в Федеральную налоговую службу в соответствующих декларациях:

– n_f – налог на прибыль организации (сумма указывается в декларации по форме КНД 1151006, код строки 190 для федерального бюджета);

– n_s – налог на прибыль организации (сумма указывается в декларации(ях) по форме КНД 1151006, приложение № 5, код строки 070 для бюджетов субъектов Российской Федерации).

Используя максимально допустимый период простоя (Δt_{MAO}, календарных дней), закрепленный в локальных актах оператора связи, с учетом условий договора возмездного оказа-

ния услуг между абонентом и оператором связи[29], осуществляется расчет значения потенциально возможного ущерба бюджетам Российской Федерации, исходя из того, что рассматривается самый худший сценарий, т.е. оператор связи в этот период с учетом условий договора не оказывает возмездные услуги электросвязи и не получает прибыль:

– значение для федерального бюджета Российской Федерации: $n_f * \Delta t_{MAO} / 365$ (тыс. рублей);

– значение для бюджета соответствующего субъекта Российской Федерации, в котором оператор связи имеет обособленное подразделение в соответствии с Налоговым кодексом Российской Федерации [14] и в котором расположена зона обслуживания конкретного объекта КИИ[30]: $n_s * \Delta t_{MAO} / 365$ (тыс. рублей).

Сопоставляются полученные значения, отнесенные к размеру соответствующего прогнозируемого годового дохода бюджета, со значениями (диапазонами значений), приведенными в таблице ниже для показателя «Возникновение ущерба бюджетам Российской Федерации» (см. Таблица 8), для каждого конкретного объекта КИИ с учетом его зоны обслуживания (субъекта Российской Федерации).

Таблица 8 – Значения показателей «Возникновение ущерба бюджетам Российской Федерации»

№	Наименование показателя	III категория	II категория	I категория
Возникновение ущерба бюджетам Российской Федерации, оцениваемого				
1.	а) в снижении доходов федерального бюджета (процентов прогнозируемого годового дохода бюджета)	более 0,001, но менее или равно 0,05	более 0,05, но менее или равно 0,1	более 0,1
2.	б) в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета)	более 0,001, но менее или равно 0,05	более 0,05, но менее или равно 0,1	более 0,1
3.	в) в снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)	Не возникает снижение доходов бюджетов государственных внебюджетных фондов вследствие компьютерных атак на объект КИИ		

[29] Учитываются условия авансирования оказания услуг, отсрочки платежа, возмещения средств абоненту и т.п., а также согласованные временные показатели для ремонтных, регламентных работ и форс-мажорных обстоятельств.
[30] Если зона обслуживания конкретного объекта КИИ покрывает несколько субъектов Российской Федерации, то рассчитываются отдельные значения для каждого субъекта Российской Федерации.

С учетом положений Федерального закона о федеральном бюджете на 2019 год [13] пороговые значения для федерального бюджета Российской Федерации, оцененные в тысячах рублей, приведены в таблице ниже (см. Таблица 9). Актуальные сведения (законы и законопроекты) о прогнозируемом годовом доходе бюджета соответствующего субъекта Российской Федерации доступны на веб-сайте: https://rg.ru.

Таблица 9 – Пороговые значений для федерального бюджета (тыс. рублей)

№	Год[31]	Прог. общий объем дохода, тыс. руб.	0,001% от прогн. общего объема дохода, тыс. руб.	0,05% от прогн. общего объема дохода, тыс. руб.	0,1% от прогн. общего объема дохода, тыс. руб.
1.	2019	19 969 336 961	199 693	9 984 668	19 969 337
2.	2020	20 218 609 435	202 186	10 109 305	20 218 609
3.	2021	20 978 007 777	209 780	10 489 004	20 978 008

3.4. При условии наличия действующего соответствующего государственного контракта на оказание услуг связи органу государственной власти (см. Приложение Б) проверяется наличие в зоне обслуживания конкретным объектом КИИ данного органа государственной власти. Только в случае, если орган государственной власти попадает в зону обслуживания конкретным объектом КИИ, сопоставляется уровень данного органа государственной власти со значениями, приведенными в таблице ниже для показателя «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» (см. Таблица 10).

Таблица 10 – Значения показателей «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)»

№	Наименование показателя	III категория	II категория	I категория
4.	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	Прекращение или нарушение функционирования органа государственной власти субъекта Российской Федерации или города федерального значения	Прекращение или нарушение функционирования федерального органа государственной власти	Прекращение или нарушение функционирования Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации

[31] Оператор связи выбирает значение прогнозируемого годового дохода для года следующего за годом проведения категорирования объекта КИИ (например, если категорирование проводится в 2019 году, то выбираются значения бюджета для 2020 года).

9 Принятие решения об установлении категории значимости объекту критической информационной инфраструктуры

Принятие решения об установлении категории значимости конкретному объекту КИИ, принадлежащему оператору связи, осуществляется оператором связи на базе значения оценки масштаба возможных последствий в случае возникновения компьютерных инцидентов на объекте КИИ (см. Рисунок 5), исходя из того, что Правилами [3] устанавливаются 3 категории значимости: самая высокая категория – первая, самая низкая – третья.

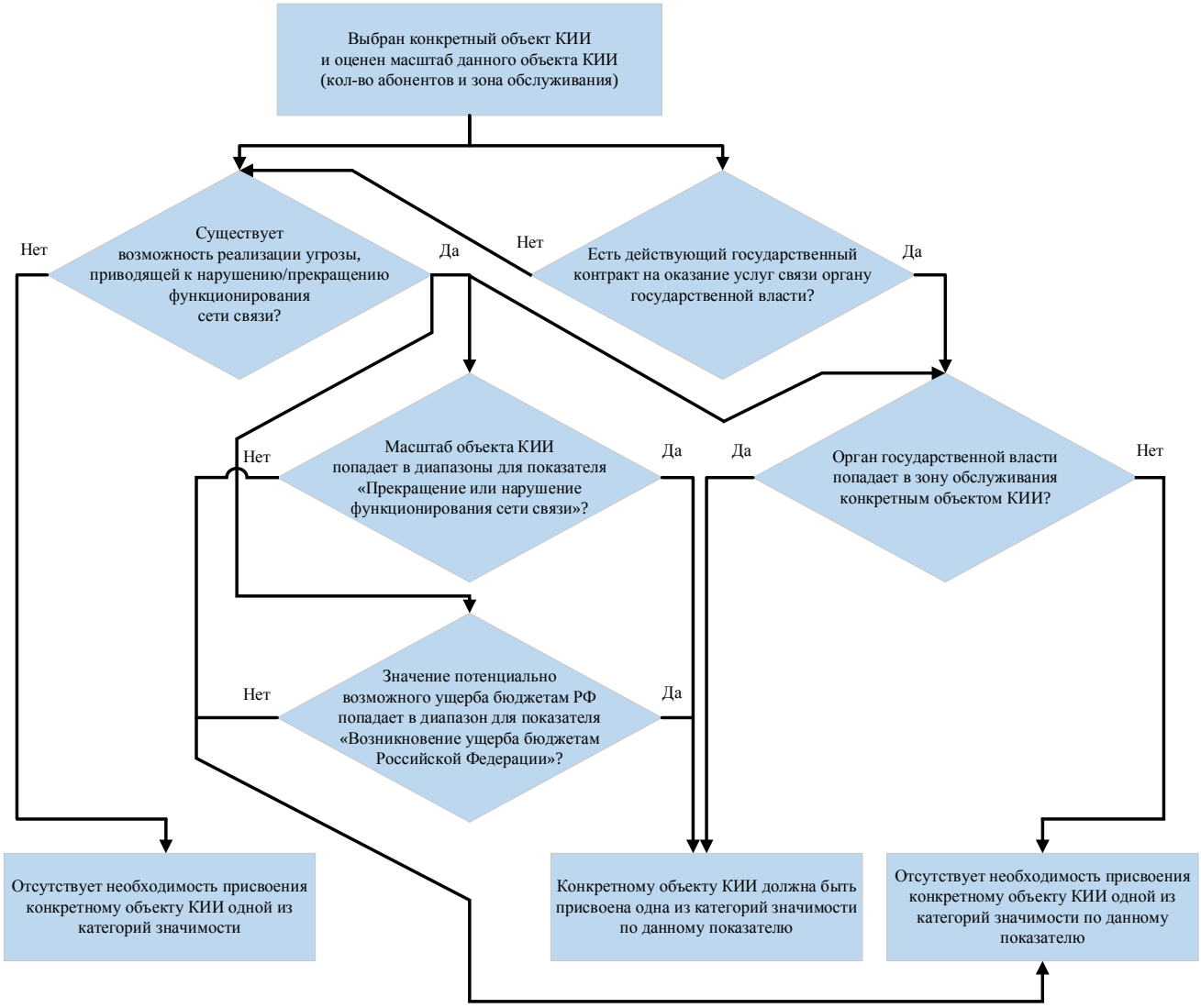

Рисунок 5 – Блок-схема подготовки к принятию решения
о присвоении категории значимости объекту КИИ

Оценка производится по каждому из значений показателя критериев значимости («Прекращение или нарушение функционирования сети связи», «Возникновение ущерба бюджетам Российской Федерации» и «Прекращение или нарушение функционирования государ-

ственного органа в части невыполнения возложенной на него функции (полномочия)»[32]), а категория значимости присваивается объекту КИИ по наивысшему значению одного из этих показателей. Обоснование неприменимости остальных показателей из Перечня [3] приведено в приложении (см. Приложение Ж).

Решение комиссии по каждому объекту КИИ оформляется отдельным актом.

Форма акта приведена в приложении (см. Приложение И). Все акты могут быть утверждены одним приказом руководителя оператора связи (акты будут выступать приложениями к соответствующему приказу), или каждый акт может быть утвержден по отдельности.

Оператор связи обеспечивает хранение акта (приказа об утверждении акта, в случае его наличия) до вывода из эксплуатации объекта КИИ или до изменения его категории значимости согласно части 12 статьи 7 Федерального закона N 187-ФЗ [2].

Рекомендации по заполнению содержательной части формы направления сведений о результатах категорирования [27] для типовых объектов КИИ, принадлежащих операторам связи, в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, приведены в приложении (см. Приложение К).

[32] Если по решению оператора связи были дополнительно рассмотрены и другие виды негативных последствий и связанные с ними показатели критериев значимости объектов КИИ, приведенные в Перечне [3], то производится оценка по каждому из значений дополнительно выбранных показателей критериев значимости.

Список использованных источников

1. Федеральный закон от 07.07.2003 N 126-ФЗ «О связи».
2. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
3. Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утв. постановлением Правительства Российской Федерации от 08.02.2018 N 127.
4. Требования к оказанию услуг подвижной радиосвязи и радиотелефонной связи при использовании бизнес-моделей виртуальных сетей подвижной радиосвязи и радиотелефонной связи, утв. приказом Министерства связи и массовых коммуникаций Российской Федерации от 20.10.2017 N 570.
5. Перечень наименований услуг связи, вносимых в лицензии на осуществление деятельности в области оказания услуг связи, утв. постановлением Правительства Российской Федерации от 18.02.2005 N 87.
6. Положение о создании (назначении) в организациях структурных подразделений (работников), уполномоченных на решение задач в области гражданской обороны, утв. постановлением Правительства Российской Федерации от 10.07.1999 N 782.
7. ГОСТ Р 53633.0-2009 «Информационные технологии (ИТ). Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Общая структура бизнес-процессов».
8. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ.
9. Правила оказания телематических услуг связи, утв. постановлением Правительства Российской Федерации от 10.09.2007 N 575.
10. Правила оказания услуг связи по передаче данных, утв. постановлением Правительства Российской Федерации от 23.01.2006 N 32.
11. Правила оказания услуг телефонной связи, утв. постановлением Правительства Российской Федерации от 09.12.2014 N 1342.
12. Концепция управления качеством связи в Российской Федерации. Министерство связи и массовых коммуникаций Российской Федерации (проект).
13. Федеральный закон от 29.11.2018 N 459-ФЗ «О федеральном бюджете на 2019 год и на плановый период 2020 и 2021 годов».
14. Налоговый кодекс Российской Федерации от 31.07.1998 N 146-ФЗ.

15. Основных направлений бюджетной, налоговой и таможенно-тарифной политики на 2019 год и на плановый период 2020 и 2021 годов. Министерство финансов Российской Федерации (проект).

16. Федеральный закон от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

17. ГОСТ Р 53633.2-2009 «Декомпозиция и описания процессов. Процессы уровня 2 eTOM. Основная деятельность. Управление и эксплуатация ресурсов».

18. ГОСТ Р 53633.4-2015 «Декомпозиция и описания процессов. Процессы уровня 2 eTOM. Основная деятельность. Управление и эксплуатация услуг».

19. ГОСТ Р 53801-2010 «Связь федеральная. Термины и определения».

20. Правила применения автоматизированных систем расчетов, утв. приказом Министерства информационных технологий и связи Российской Федерации от 02.07.2007 N 73.

21. Перечень средств связи, подлежащих обязательной сертификации, утв. постановлением Правительства Российской Федерации от 25.06.2009 N 532.

22. Правила применения оборудования автоматизированных систем управления и мониторинга сетей электросвязи. Часть IV. Правила применения оборудования выделенных транзитных пунктов сигнализации, утв. приказом Министерства связи и массовых коммуникаций Российской Федерации от 30.10.2009 N 136.

23. РД 45.174-2001 «Построение систем управления сетями связи операторов взаимоувязанной сети связи Российской Федерации. Основные положения».

24. Рекомендуемая форма перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию, приложение 1 к информационному сообщению ФСТЭК России от 24.08.2018 N 240/25/3752.

25. Требования к порядку ввода сетей электросвязи в эксплуатацию, утв. приказом Министерства связи и массовых коммуникаций Российской Федерации от 26.08.2014 N 258.

26. ГОСТ Р 53633.2-2009 «Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности».

27. Форма направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утв. приказом ФСТЭК России от 22.12.2017 N 236.

28. ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения».

29. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утв. приказом ФСТЭК России от 18.05.2007.

Приложение А

Рекомендуемая форма приказа о создании комиссии по категорированию объектов критической информационной инфраструктуры, принадлежащих операторам связи

№ ____ от __.__.____

ПРИКАЗ
о создании комиссии по категорированию

С целью организации и проведения работ по категорированию объектов критической информационной инфраструктуры

ПРИКАЗЫВАЮ:

1. Создать постоянно действующую комиссию по категорированию объектов критической информационной инфраструктуры, принадлежащих *название оператора связи* на праве собственности, аренды или ином законном основании.
2. Председателем комиссии назначить *должность, ФИО*.
3. В состав комиссии включить:
   - *должность, ФИО*;
   - …
   - *должность, ФИО*.
4. Комиссии в срок до *ДД.ММ.ГГГГ*:

– определить процессы в рамках осуществления видов деятельности *название оператора связи*;

– выявить критические процессы у *название оператора связи*;

– выявить объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

– подготовить предложения для включения объектов критической информационной инфраструктуры в перечень объектов критической информационной инфраструктуры, подлежащих категорированию;

– представить на утверждение перечень объектов критической информационной инфраструктуры, подлежащих категорированию, в срок до *ДД.ММ.ГГГГ*;

– рассмотреть возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

– проанализировать угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;

– оценить в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

– установить каждому из объектов критической информационной инфраструкту-

ры одну из категорий значимости либо принять решение об отсутствии необходимости присвоения им категорий значимости;

– представить на утверждение акты по результатам категорирования;

– представить на утверждение сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

5. Комиссии в своей деятельности руководствоваться положениями действующих нормативно-правовых и методических документов:

– Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. N 187-ФЗ (ст. 7);

– Правила категорирования объектов критической информационной инфраструктуры Российской Федерации и Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. N 127;

– Форма направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденные приказом ФСТЭК России от 22 декабря 2017 г. N 236;

– Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи, Ассоциации Документальной Электросвязи 2018 г.

6. Ознакомить с настоящим приказом председателя и членов создаваемой комиссии.

7. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель оператора связи *И.О. Фамилия*

Приложение Б

Перечень органов государственной власти

Таблица 11 – Значение показателя для I категории

№	Наименование органа государственной власти
1.	Администрация Президента Российской Федерации
2.	Правительство Российской Федерации
3.	Федеральное Собрание Российской Федерации
4.	Совет Безопасности Российской Федерации
5.	Верховный Суд Российской Федерации
6.	Конституционный Суд Российской Федерации

Таблица 12 – Значение показателя для II категории

№	Наименование федерального органа государственной власти[33]
1.	Министерство внутренних дел Российской Федерации
2.	Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий
3.	Министерство иностранных дел Российской Федерации
4.	Федеральное агентство по делам Содружества Независимых Государств, соотечественников, проживающих за рубежом, и по международному гуманитарному сотрудничеству
5.	Министерство обороны Российской Федерации
6.	Федеральная служба по военно-техническому сотрудничеству
7.	Федеральная служба по техническому и экспортному контролю
8.	Министерство юстиции Российской Федерации
9.	Федеральная служба исполнения наказаний
10.	Федеральная служба судебных приставов
11.	Государственная фельдъегерская служба Российской Федерации (федеральная служба)
12.	Служба внешней разведки Российской Федерации (федеральная служба)
13.	Федеральная служба безопасности Российской Федерации (федеральная служба)
14.	Федеральная служба войск национальной гвардии Российской Федерации (федеральная служба)
15.	Федеральная служба охраны Российской Федерации (федеральная служба)
16.	Федеральная служба по финансовому мониторингу (федеральная служба)
17.	Федеральное архивное агентство (федеральное агентство)

[33] Федеральные органы исполнительной власти в соответствии с Указом Президента Российской Федерации «О структуре федеральных органов исполнительной власти» от 15.05.2018 г. N 215. Федеральные суды в соответствии с Федеральным конституционным законом от 31.12.1996 N 1-ФКЗ «О судебной системе Российской Федерации», кроме Верховного суда Российской Федерации и Конституционного суда Российской Федерации.

№	Наименование федерального органа государственной власти[33]
18.	Главное управление специальных программ Президента Российской Федерации (федеральное агентство)
19.	Управление делами Президента Российской Федерации (федеральное агентство)
20.	Министерство здравоохранения Российской Федерации
21.	Федеральная служба по надзору в сфере здравоохранения
22.	Федеральное медико-биологическое агентство
23.	Министерство культуры Российской Федерации
24.	Позиция исключена. - Указ Президента РФ от 14.09.2018 N 514
25.	Министерство науки и высшего образования Российской Федерации
26.	Министерство природных ресурсов и экологии Российской Федерации
27.	Федеральная служба по гидрометеорологии и мониторингу окружающей среды
28.	Федеральная служба по надзору в сфере природопользования
29.	Федеральное агентство водных ресурсов
30.	Федеральное агентство лесного хозяйства
31.	Федеральное агентство по недропользованию
32.	Министерство промышленности и торговли Российской Федерации
33.	Федеральное агентство по техническому регулированию и метрологии
34.	Министерство просвещения Российской Федерации
35.	Министерство Российской Федерации по развитию Дальнего Востока
36.	Министерство Российской Федерации по делам Северного Кавказа
37.	Министерство сельского хозяйства Российской Федерации
38.	Федеральная служба по ветеринарному и фитосанитарному надзору
39.	Федеральное агентство по рыболовству
40.	Министерство спорта Российской Федерации
41.	Министерство строительства и жилищно-коммунального хозяйства Российской Федерации
42.	Министерство транспорта Российской Федерации
43.	Федеральная служба по надзору в сфере транспорта
44.	Федеральное агентство воздушного транспорта
45.	Федеральное дорожное агентство
46.	Федеральное агентство железнодорожного транспорта
47.	Федеральное агентство морского и речного транспорта
48.	Министерство труда и социальной защиты Российской Федерации
49.	Федеральная служба по труду и занятости
50.	Министерство финансов Российской Федерации
51.	Федеральная налоговая служба
52.	Федеральная служба по регулированию алкогольного рынка
53.	Федеральная таможенная служба
54.	Федеральное казначейство (федеральная служба)
55.	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

№	Наименование федерального органа государственной власти[33]
56.	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
57.	Федеральное агентство по печати и массовым коммуникациям
58.	Федеральное агентство связи
59.	Министерство экономического развития Российской Федерации
60.	Федеральная служба по аккредитации
61.	Федеральная служба государственной регистрации, кадастра и картографии
62.	Федеральная служба государственной статистики
63.	Федеральная служба по интеллектуальной собственности
64.	Федеральное агентство по туризму
65.	Федеральное агентство по управлению государственным имуществом
66.	Министерство энергетики Российской Федерации
67.	Федеральная антимонопольная служба
68.	Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека
69.	Федеральная служба по надзору в сфере образования и науки
70.	Федеральная служба по экологическому, технологическому и атомному надзору
71.	Федеральное агентство по государственным резервам
72.	Федеральное агентство по делам молодежи
73.	Федеральное агентство по делам национальностей
74.	Кассационные суды общей юрисдикции
75.	Апелляционные суды общей юрисдикции
76.	Верховные суды республик
77.	Краевые суды
78.	Областные суды
79.	Суды городов федерального значения
80.	Суды автономной области
81.	Суды автономных округов
82.	Районные суды
83.	Военные суды
84.	Специализированные суды, составляющие систему федеральных судов общей юрисдикции
85.	Арбитражные суды округов
86.	Арбитражные апелляционные суды
87.	Арбитражные суды субъектов Российской Федерации
88.	Специализированные арбитражные суды, составляющие систему федеральных арбитражных судов

Таблица 13 –Значение показателя для III категории

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
1.	Республика Адыгея (Адыгея)	Государственный Совет - Хасэ Республики Адыгея
		Кабинет Министров Республики Адыгея
		Суды Республики Адыгея, в соответствии с Конституцией Республики Адыгея от 10.03.1995 г.
2.	Республика Алтай	Государственное Собрание - Эл Курултай Республики Алтай
		Правительство Республики Алтай
		Суды Республики Алтай, в соответствии с Конституцией Республики Алтай от 07.06.1997 г.
3.	Республика Башкортостан	Государственное Собрание Республики Башкортостан
		Правительство Республики Башкортостан
		Местные органы государственной власти Республики Башкортостан
		Суды Республики Башкортостан, в соответствии с Конституцией Республики Башкортостан от 24.12.1993 г.
4.	Республика Бурятия	Народный Хурал Республики Бурятия
		Правительство Республики Бурятия
		Суды Республики Бурятия, в соответствии с Конституцией Республики Бурятия от 22.02.1994 г.
5.	Республика Дагестан	Народное Собрание Республики Дагестан
		Правительство Республики Дагестан
		Суды Республики Дагестан, в соответствии с Конституцией Республики Дагестан от 10.03.2003 г.
6.	Республика Ингушетия	Народное Собрание (Парламент) Республики Ингушетия
		Правительство Республики Ингушетия, республиканские и территориальные органы исполнительной власти Республики Ингушетия
		Конституционный Суд Республики Ингушетия и мировые судьи Республики Ингушетия, в соответствии с Конституцией Республики Ингушетия от 27.02.1994 г.
7.	Кабардино-Балкарская Республика	Парламент Кабардино-Балкарской Республики
		Правительство Кабардино-Балкарской Республики
		Суды Кабардино-Балкарской Республики, в соответствии с Конституцией Кабардино-Балкарской Республики от 01.09.1997 г.
8.	Республика Калмыкия	Народный Хурал (Парламент) Республики Калмыкия
		Правительство Республики Калмыкия

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
		Верховный суд Республики Калмыкия, Арбитражный суд Республики Калмыкия, районные суды и мировые судьи Республики Калмыкия, в соответствии с Степным Уложением (Конституцией) Республики Калмыкия от 05.04.1994 г.
9.	Карачаево-Черкесская Республика	Народное Собрание (Парламент) Карачаево-Черкесской Республики
		Правительство Карачаево-Черкесской Республики
		суды Карачаево-Черкесской Республики, в соответствии с Конституцией Карачаево-Черкесской Республики от 05.03.1996 г.
10.	Республика Карелия	Законодательное Собрание Республики Карелия
		Правительство Республики Карелия и иные органы исполнительной власти
		суды Республики Карелия, в соответствии с Конституцией Республики Карелия от с 07.02.2001 г.
11.	Республика Коми	Государственный Совет Республики Коми
		Правительство Республики Коми и иные органы исполнительной власти Республики Коми
		Конституционный Суд Республики Коми и мировые судьи, в соответствии с Конституцией Республики Коми от 17.02.1994 г.
12.	Республика Крым	Государственный Совет Республики Крым – Парламент Республики Крым
		Совет министров Республики Крым – Правительство Республики Крым
		Суды Республики Крым, в соответствии с Конституцией Республики Крым от 11.04.2014 г.
13.	Республика Марий Эл	Государственное Собрание Республики Марий Эл
		Правительство Республики Марий Эл
		Конституционный Суд Республики Марий Эл и иные органы, в соответствии с Конституцией Республики Марий Эл от 24.06.1995 г.
14.	Республика Мордовия	Государственное Собрание Республики Мордовия
		Правительство Республики Мордовия и иные исполнительные органы государственной власти Республики Мордовия
		Суды Республики Мордовия, в соответствии с Конституцией Республики Мордовия от 21.09.1995 г.
15.	Республика Саха (Якутия)	Государственное Собрание (Ил Тумэн) Республики Саха (Якутия)
		Администрация Главы Республики Саха (Якутия) и Правительства Республики Саха (Якутия)
		Конституционный суд Республики Саха (Якутия)
16.	Республика Северная	Парламент Республики Северная Осетия-Алания
		Правительство Республики Северная Осетия-Алания

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
	Осетия - Алания	Суды Республики Северная Осетия-Алания
		Иные органы государственной власти Республики Северная Осетия-Алания, в соответствии с Конституцией Республики Северная Осетия-Алания от 12.11.1994 г.
17.	Республика Татарстан (Татарстан)	Государственный Совет Республики Татарстан – парламент Республики Татарстан
		Кабинет Министров Республики Татарстан
		Суды Республики Татарстан, в соответствии с Конституцией Республики Татарстан от 19.04.2002 г.
18.	Республика Тыва	Верховный Хурал (парламент) Республики Тыва
		Правительство Республики Тыва
		Конституционный суд Республики Тыва и мировые судьи, в соответствии с Конституцией Республики Тыва от 06.05.2001 г.
19.	Удмуртская Республика	Государственный Совет Удмуртской Республики
		Правительство Удмуртской Республики
		Конституционный Суд Удмуртской Республики, мировые судьи Удмуртской Республики, в соответствии с Конституцией Удмуртской Республики от 07.12.1994 г.
20.	Республика Хакасия	Верховный Совет Республики Хакасия
		Правительство Республики Хакасия
		Конституционный суд Республики Хакасия, Верховный суд Республики Хакасия, Арбитражный суд Республики Хакасия, районные и другие суды, в соответствии с Конституцией Республики Хакасия от 25.05.1995 г.
21.	Чеченская Республика	Парламент Чеченской Республики
		Правительство Чеченской Республики
		Суды Чеченской Республики, в соответствии с Конституцией Чеченской Республики от 23.03.2003 г.
22.	Чувашская Республика – Чувашия	Государственный Совет Чувашской Республики
		Кабинет Министров Чувашской Республики
		Суды Чувашской Республики, в соответствии с Конституцией Чувашской Республики от 30.11.2000 г.
23.	Алтайский край	Алтайское краевое Законодательное Собрание
		Правительство Алтайского края, в соответствии с Уставом (Основным законом) Алтайского края от 26.05.1995 г.
24.	Забайкальский край	Законодательное Собрание Забайкальского края
		Правительство Забайкальского края, в соответствии с Уставом Забайкальского края от 17.02.2009 г.
25.	Камчатский край	Законодательное Собрание Камчатского края
		Правительство Камчатского края

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
		Мировые судьи в Камчатском крае и Уставный суд Камчатского края, в соответствии с Уставом Камчатского Края от 14.11.2008 г.
26.	Краснодарский край	Законодательное Собрание Краснодарского края
		Администрация Краснодарского края
		Иные органы государственной власти Краснодарского края, образуемые в соответствии с Уставом Краснодарского края от 09.06.2010 г.
27.	Красноярский край	Законодательное Собрание Красноярского края
		Правительство Красноярского края
		Иные органы исполнительной власти Красноярского края
		Мировые судьи Красноярского края, в соответствии с Уставом Красноярского края от 05.06.2008 г.
28.	Пермский край	Законодательное собрание Пермского края
		Правительство Пермского края
		Суды Пермского края
		Иные органы государственной власти, образуемые в соответствии с Уставом Пермского края от 27.04.2007 г.
29.	Приморский край	Законодательное Собрание Приморского края
		Администрация Приморского края
		Иные органы исполнительной власти Приморского края, формируемые Администрацией Приморского края, в соответствии с Уставом Приморского края от 06.10.1995 г.
30.	Ставропольский край	Дума Ставропольского края
		Правительство Ставропольского края
		Суды Ставропольского края, в соответствии с Уставом Ставропольского края от 12.10.1994 г.
31.	Хабаровский край	Законодательная Дума Хабаровского края
		Правительство Хабаровского края
		Суды Хабаровского края, в соответствии с Уставом Хабаровского края от 30.11.1995 г.
32.	Амурская область	Законодательное Собрание Амурской области
		Правительство Амурской области
		Иные органы исполнительной власти области
		Уставный суд Амурской области
		Мировые судьи области, в соответствии с Уставом (Основным законом) Амурской области от 13.12.1995 г.
33.	Архангельская область	Архангельское областное Собрание депутатов
		Правительство Архангельской области
		Избирательная комиссия Архангельской области
		Контрольно-счетная палата Архангельской области

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
		Уполномоченный по правам человека в Архангельской области и другие государственные органы Архангельской области, в соответствии с Уставом Архангельской области от 23.05.1995 г.
34.	Астраханская область	Дума Астраханской области
		Правительство Астраханской области
		иные исполнительные органы государственной власти Астраханской области, образуемые в соответствии с Уставом Астраханской области от 29.03.2007 г.
35.	Белгородская область	Белгородская областная Дума
		Правительство Белгородской области
		иные органы исполнительной власти Белгородской области, образуемые в соответствии с Уставом Белгородской области от 24.12.2003 г.
		Уставный суд Белгородской области и мировые судьи Белгородской области
36.	Брянская область	Брянская областная Дума
		Правительство Брянской области
		Исполнительные органы государственной власти Брянской области
		Мировые судьи Брянской области, в соответствии с Уставом Брянской области от 20.12.2012 г.
37.	Владимирская область	Законодательное Собрание Владимирской области
		Администрация Владимирской области
		Иные органы государственной власти, образуемые в соответствии с Уставом (Основным законом) Владимирской области от 14.08.2001 г.
38.	Волгоградская область	Волгоградская областная Дума
		Администрация Волгоградской области
		Иные исполнительные органы государственной власти Волгоградской области, в соответствии с Уставом (Основным законом) Волгоградской области от 14.02.2012 г.
39.	Вологодская область	Законодательное Собрание области
		Правительство области
		Органы исполнительной государственной власти области, в соответствии с Уставом Вологодской области от 03.12.2001 г.
40.	Воронежская область	Воронежская областная Дума
		Правительство Воронежской области
		Иные органы государственной власти Воронежской области, созданные в соответствии с Уставом Воронежской области от 25.05.2006 г.
41.	Ивановская	Ивановская областная Дума

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
	область	Правительство Ивановской области
		Суды Ивановской области
		Иные органы государственной власти Ивановской области, образуемые в соответствии с Уставом Ивановской области от 29.01.2009 г.
42.	Иркутская область	Законодательное Собрание Иркутской области
		Правительство Иркутской области
		министерства и иные исполнительные органы государственной власти Иркутской области
		Уставный Суд Иркутской области
		Мировые судьи Иркутской области
		Избирательная комиссия Иркутской области
		Территориальные избирательные комиссии Иркутской области
		Контрольно-счетная палата Иркутской области
		Уполномоченный по правам человека в Иркутской области
		Уполномоченный по правам ребенка в Иркутской области
		Уполномоченный по защите прав предпринимателей в Иркутской области, в соответствии с Уставом Иркутской области от 15.04.2009 г.
43.	Калининградская область	Калининградская областная Дума
		Правительство Калининградской области
		Иные исполнительные органы государственной власти Калининградской области в соответствии со структурой, определенной Губернатором Калининградской области
		Уставный Суд Калининградской области, в соответствии с Уставом (Основным законом) Калининградской области от 28.12.1995 г.
44.	Калужская область	Законодательное Собрание Калужской области
		Правительство Калужской области
		Иные органы государственной власти Калужской области, образуемые в соответствии с Уставом Калужской области от 27.03.1996 г.
45.	Кемеровская область	Совет народных депутатов Кемеровской области
		Коллегия Администрации Кемеровской области
		Иные исполнительные органы государственной власти Кемеровской области
		Избирательная комиссия Кемеровской области
		Уполномоченный по правам человека в Кемеровской области
		Уполномоченный по правам ребенка в Кемеровской области
		Уполномоченный по защите прав предпринимателей в Кемеровской области

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
		Контрольно-счетная палата Кемеровской области, в соответствии с Уставом Кемеровской области от 09.04.1997 г.
46.	Кировская область	Законодательное Собрание Кировской области
		Правительство Кировской области
		Иные органы исполнительной власти Кировской области, образуемые Правительством Кировской области в соответствии с Уставом Кировской области от 29.02.1996 г.
		Уставный суд Кировской области
		Мировые судьи Кировской области
47.	Костромская область	Костромская областная Дума
		Администрация Костромской области
		Мировые судьи, действующие на территории Костромской области
		Иные органы государственной власти Костромской области, образуемые в соответствии с Уставом Костромской области от 17.04.2008 г.
48.	Курганская область	Курганская областная Дума
		Правительство Курганской области
		Органы исполнительной власти области, осуществляющие отраслевое либо межотраслевое управление
		Исполнительно-распорядительные (территориальные) органы государственной власти в городах областного подчинения Курган и Шадринск и районах области
		Суды Курганской области, в соответствии с Уставом Курганской области от 01.12.1994 г.
49.	Курская область	Курская областная Дума
		Администрация Курской области
		Иные органы государственной власти Курской области, образуемые в соответствии с Уставом Курской области от 27.09.2001 г.
50.	Ленинградская область	Законодательное собрание Ленинградской области
		Правительство Ленинградской области
		Отраслевые, территориальные и иные органы исполнительной власти Ленинградской области, входящие в состав Администрации Ленинградской области
		Уставный суд Ленинградской области
		Мировые судьи Ленинградской области, в соответствии с Уставом Ленинградской области от 27.10.1994 г.
51.	Липецкая область	Липецкий областной Совет депутатов
		Администрация Липецкой области
		Суды Липецкой области, в соответствии с Уставом Липецкой области от 27.03.2003 г.

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
52.	Магаданская область	Магаданская областная Дума
		Правительство Магаданской области
		иные органы государственной власти Магаданской области, образуемые в соответствии с Уставом Магаданской области от 26.12.2001 г.
53.	Московская область	Московская областная Дума
		Правительство Московской области
		Центральные исполнительные органы государственной власти Московской области
		Территориальные исполнительные органы государственной власти Московской области
		Уставный суд Московской области, в соответствии с Уставом Московской области от 04.12.1996 г.
54.	Мурманская область	Мурманская областная Дума
		Правительство Мурманской области
		иные органы государственной власти, образуемые в соответствии с Уставом Мурманской области от 26.11.1997 г.
55.	Нижегородская область	Законодательное Собрание Нижегородской области
		Правительство Нижегородской области
		Министерства и иные органы исполнительной власти области
		Мировые судьи и Уставный суд Нижегородской области, в соответствии с Уставом Нижегородской области от 22.12.2005 г.
56.	Новгородская область	Новгородская областная Дума
		Правительство Новгородской области
		Суды Новгородской области, в соответствии с Уставом Новгородской области от 31.08.1994 г.
57.	Новосибирская область	Законодательное Собрание Новосибирской области
		Правительство Новосибирской области
		Суды Новосибирской области, в соответствии с Уставом Новосибирской области от 18.04.2005 г.
58.	Омская область	Законодательное Собрание Омской области
		Правительство Омской области
		Суды Омской области, в соответствии с Уставом (Основным законом) Омской области от 26.12.1995 г.
59.	Оренбургская область	Законодательное Собрание Оренбургской области
		Правительство Оренбургской области
		Суды Оренбургской области, в соответствии с Уставом (Основным законом) Оренбургской области от 25.10.2000 г.
60.	Орловская область	Орловский областной Совет народных депутатов
		Правительство Орловской области

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
		Органы исполнительной государственной власти специальной компетенции Орловской области
		Суды Орловской области, в соответствии с Уставом (Основным законом) Орловской области от 26.02.1996 г.
61.	Пензенская область	Законодательное Собрание Пензенской области
		Правительство Пензенской области
		Иные исполнительные органы государственной власти (иные органы исполнительной власти) Пензенской области - в соответствии с их системой, устанавливаемой законом Пензенской области
		Мировые судьи в Пензенской области
		Счетная палата Пензенской области
		Избирательная комиссия Пензенской области
		Иные государственные органы Пензенской области, в соответствии с Уставом Пензенской области от 10.09.1996 г.
62.	Псковская область	Псковское областное Собрание депутатов
		Администрация Псковской области
		Иные органы исполнительной власти области, формируемые Администрацией области, в соответствии с Уставом Псковской области от 29.03.2001 г.
63.	Ростовская область	Законодательное Собрание Ростовской области
		Правительство Ростовской области
		иные органы государственной власти Ростовской области, образуемые в соответствии с Уставом Ростовской области от 19.04.1996 г.
64.	Рязанская область	Рязанская областная Дума
		Правительство Рязанской области
		иные органы государственной власти Рязанской области, образуемые в соответствии с Уставом Рязанской области от 02.11.2005 г.
65.	Самарская область	Самарская Губернская Дума
		Правительство Самарской области
		Министерства Самарской области
		Иные органы исполнительной власти Самарской области
		Суды Самарской области, в соответствии с Уставом Самарской области от 05.12.2006 г.
66.	Саратовская область	Саратовская областная Дума
		Правительство Саратовской области
		Иные органы государственной власти Самарской области, в соответствии с Уставом Самарской области от 24.05.2005 г.
67.	Сахалинская область	Сахалинская областная Дума
		Правительство Сахалинской области

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
		Суды Сахалинской области, в соответствии с Уставом Сахалинской области от 28.06.2001 г.
68.	Свердловская область	Законодательное Собрание Свердловской области
		Правительство Свердловской области
		Иные исполнительные органы государственной власти Свердловской области
		Уставный Суд Свердловской области
		Мировые судьи Свердловской области, в соответствии с Уставом Свердловской области от 16.12.2010 г.
69.	Смоленская область	Смоленская областная Дума
		Администрация Смоленской области
		Мировые судьи Смоленской области
		Иные органы государственной власти Смоленской области, созданные в соответствии с Уставом Смоленской области от 26.04.2001 г.
70.	Тамбовская область	Тамбовская областная Дума
		Администрация Тамбовской области
		Суды Тамбовской области, в соответствии с Уставом (Основным законом) Тамбовской области от 30.11.1994 г.
71.	Тверская область	Законодательное Собрание Тверской области
		Правительство Тверской области
		Уставный суд Тверской области
		Мировые судьи Тверской области, в соответствии с Уставом Тверской области от 05.11.1996 г.
72.	Томская область	Законодательная Дума Томской области
		Администрация Томской области
		Суды Томской области, в соответствии с Уставом Томской области от 26.07.1995 г.
73.	Тульская область	Тульская областная Дума
		Правительство Тульской области, в соответствии с Уставом Тульской области от 28.05.2015 г.
74.	Тюменская область	Тюменская областная Дума
		Правительство Тюменской области
		Иные органы государственной власти, образуемые в соответствии с Уставом Тульской области от 15.06.1995 г.
75.	Ульяновская область	Законодательное собрание Ульяновской области
		Правительство Ульяновской области
		иные органы государственной власти Ульяновской области, образуемые в соответствии с Уставом Ульяновской области от 19.05.2005 г.
76.	Челябинская	Законодательное Собрание Челябинской области

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
	область	Правительство Челябинской области
		Иные органы исполнительной власти Челябинской области
		Мировые судьи Челябинской области, в соответствии с Уставом (Основным законом) Челябинской области от 25.05.2006 г.
77.	Ярославская область	Ярославская областная Дума
		Правительство Ярославской области
		Иные органы исполнительной власти Ярославской области, в соответствии с Уставом Ярославской области от 28.09.2010 г.
78.	Москва	Московская городская Дума
		Правительство Москвы
		Уставный суд города Москвы
		Мировые судьи города Москвы, в соответствии с Уставом города Москвы от 28.06.1995 г.
79.	Санкт-Петербург	Законодательное Собрание Санкт-Петербурга
		Правительство Санкт-Петербурга
		Иные исполнительные органы государственной власти Санкт-Петербурга, составляющие систему исполнительных органов государственной власти Санкт-Петербурга - Администрацию Санкт-Петербурга
		Уставный суд Санкт-Петербурга
		Мировые судьи Санкт-Петербурга, в соответствии с Уставом города Санкт-Петербурга от 14.01.1998 г.
80.	Севастополь	Законодательное Собрание города Севастополя
		Правительство Севастополя, в соответствии с Уставом города Севастополя от 11.04.2014 г.
81.	Еврейская автономная область	Законодательное Собрание Еврейской автономной области
		Правительство Еврейской автономной области
		Суды Еврейской автономной области, в соответствии с Уставом Еврейской автономной области от 08.10.1997 г.
82.	Ненецкий автономный округ	Собрание депутатов Ненецкого автономного округа
		Администрация Ненецкого автономного округа
		Иные органы государственной власти Ненецкого автономного округа, образуемые в соответствии с Уставом Ненецкого автономного округа от 11.09.1995 г.
83.	Ханты-Мансий-	Дума Ханты-Мансийского автономного округа - Югры
		Правительство Ханты-Мансийского автономного округа - Югры

№	Субъект Российской Федерации	Наименование органа государственной власти субъекта Российской Федерации или города федерального значения
	ский автономный округ – Югра	Государственные органы Ханты-Мансийского автономного округа – Югры, в соответствии с Уставом Ханты-Мансийского автономного округа – Югры от 26.04.1995 г.
84.	Чукотский автономный округ	Дума Чукотского автономного округа
		Правительство Чукотского автономного округа
		иные органы государственной власти Чукотского автономного округа, образуемые в соответствии с Уставом Чукотского автономного округа от 29.10.1997 г.
85.	Ямало-Ненецкий автономный округ	Законодательное Собрание Ямало-Ненецкого автономного округа
		Правительство Ямало-Ненецкого автономного округа
		Иные исполнительные органы государственной власти автономного округа, образованные в соответствии с Уставом Ямало-Ненецкого автономного округа от 27.12.1998 г.
		Уставный суд Ямало-Ненецкого автономного округа
		Мировые судьи Ямало-Ненецкого автономного округа

Приложение В

Перечень типовых информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, принадлежащих операторам связи

Таблица 14 – Перечень типовых ИС, ИТКС и АСУ, принадлежащих операторам связи

№	Наименование	Назначение
1.	**Информационные системы**[34]	
1.1.	Блок бизнеса (Business Support Systems (BSS))	
1.1.1.	Автоматизированные системы расчетов / Биллинговые системы (Billing)	1. Автоматизация расчетов с абонентами за любые виды оказываемых им или заказываемых ими услуг связи в любом сочетании за исключением услуг связи, оказываемых с использованием таксофонов, услуг телеграфной связи и услуг почтовой связи. 2. Автоматизация предобработки информации об оказанных услугах связи (пребиллинг). 3. Автоматизация задач активации продуктов и услуг связи. 4. Автоматизация задач предоставления услуг связи (в т.ч. ограничения предоставления услуг связи) для предоплатной модели расчетов («prepaid»). 5. Информационное обеспечение работников оператора связи сведениями для предоставления абоненту информации об оказанных услугах связи по запросу (в т.ч. выдача на твердую копию). 6. Информационное обеспечение работников оператора связи в рамках проведения взаиморасчетов между операторами связи. 7. Хранение данных о состоянии счетов абонентов
1.1.2.	Системы самообслуживания абонентов	1. Автоматизация задач управления набором услуг, предоставляемых абонентам. 2. Автоматизация задач подключения/отключения дополнительных услуг, смены тарифного плана абонентом. 3. Информационное обеспечение абонента справочными сведениями, в т.ч. о состоянии его лицевого счета (баланса)
1.1.3.	Системы информационно-справочного обслуживания абонентов	1. Информационное обеспечение пользователя и/или абонента справочными сведениями, связанными с оказанием услуг связи (в т.ч. сведения о тарифах, состоя-

[34] Здесь и далее под назначением информационных систем понимается информационное обеспечение и автоматизация процессов в рамках видов деятельности, осуществляемых операторами связи.

№	Наименование	Назначение
		нии лицевого счета и др.). 2. Предоставление сведений об операторе связи, а также информации, необходимой для заключения и исполнения договора между оператором связи и абонентом
1.1.4.	Системы планирования ресурсов предприятия (Enterprise Resource Planning (ERP))	1. Автоматизация задач управления финансами, бухгалтерский, налоговый учет. 2. Автоматизация задач управления трудовыми ресурсами. 3. Автоматизация задач управления проектами. 4. Автоматизация задач управления активами. 5. Автоматизация задач управления закупками. 6. Информационное обеспечение работников оператора связи
1.1.5.	Системы управления взаимоотношениями с абонентами	
1.1.5.1.	Системы управления абонентским обслуживанием (Customer Relationship Management (CRM))	1. Автоматизация обработки и предоставления данных об абонентах оператора связи, в т.ч. в другие системы оператора связи. 2. Автоматизация задач удаленных продаж. 3. Автоматизация задач подключения и обслуживания абонентов из удаленных офисов партнеров, сервис-провайдеров и филиалов оператора связи
1.1.5.2.	Системы обработки обращений пользователей услуг связи (Call)	1. Автоматизация задач контроля качества обслуживания пользователей услуг связи. 2. Информационное обеспечение работников оператора связи в рамках контроля качества обслуживания пользователей услуг связи (запись, хранение, воспроизведение и автоматизация анализа аудио и видео информации)
1.2.	Блок поддержки (Operations Support Systems (OSS))	
1.2.1.	Сервисные шины предприятия (Enterprise service bus (ESB)) / Интеграционные среды	Автоматизация обмена сообщениями между различными информационными системами, корпоративными приложениями оператора связи
1.2.2.	Системы обнаружения мошенничества (Antifraud)	1. Автоматизация задач защиты доходов. 2. Автоматизация задач по выявлению аномалий. 3. Автоматизация и информационное обеспечение работников оператора связи в рамках задач управления потерями. 4. Автоматизация и информационное обеспечение работников оператора связи в рамках задач управления деятельностью и событиями, связанными со счетами абонентов и оплатами счетов. 5. Информационное обеспечение задач работников опе-

№	Наименование	Назначение
		ратора связи, направленных на ограничение предоставления услуг связи (SMS-рассылки, мобильный банк и др.)
1.3.	Системы оперативно-розыскных мероприятий (СОРМ)	Информационное обеспечение работников органов обеспечения правопорядка и безопасности в рамках проведения оперативно-розыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи (хранение текстовых сообщений абонентов, голосовой информации, изображений, звуков, видео или иных сообщений абонентов, а также хранение информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео или иных сообщений абонентов)
2.	**Информационно-телекоммуникационные сети**	
2.1.	Выделенные сети передачи данных для управления и мониторинга сетей электросвязи (Data Communication Network (DCN))	Передача информации между автоматизированными системами управления и мониторинга сетей связи и средствами связи
2.2.	Локальные вычислительные сети (ЛВС)	Передача информации между программными и техническими средствами оператора связи, предназначенными для решения задач оператора связи и расположенными на небольшой территории (например, в здании, предприятии, учреждении)
3.	**Автоматизированные системы управления**	
3.1.	Автоматизированные системы управления и мониторинга сетей электросвязи / Системы управления сетью (Network Management Systems (NMS))	1. Автоматизация и информационное обеспечение работников оператора связи в рамках задач управления неисправностями (инцидентами), контроль выполнения задач по устранению неисправностей. 2. Автоматизация и информационное обеспечение работников оператора связи в рамках задач мониторинга. 3. Автоматизация и информационное обеспечение работников оператора связи в рамках задач управления конфигурациями. 4. Автоматизация и информационное обеспечение работников оператора связи в рамках задач управления производительностью. 5. Автоматизация и информационное обеспечение работников оператора связи в рамках задач управления изменениями.

№	Наименование	Назначение
		6. Автоматизация инвентаризации и технического учета
3.2.	Выделенные транзитные пункты сигнализации (Signalling Transfer Point (STP) / Diameter Routing Agent (DRA))	1. Управление сетью сигнализации, обработка сообщений сигнализации. 2. Передача сигнального трафика, маршрутизация сигнальных сообщений. 3. Сбор статистики сигнальных сообщений. 4. Защита от несанкционированного доступа в сеть общеканальной сигнализации N 7 (ОКС N 7). 5. Учет сигнального трафика для взаиморасчетов между операторами связи

Приложение Г

Логические схемы типовых объектов критической информационной инфраструктуры, принадлежащих операторам связи

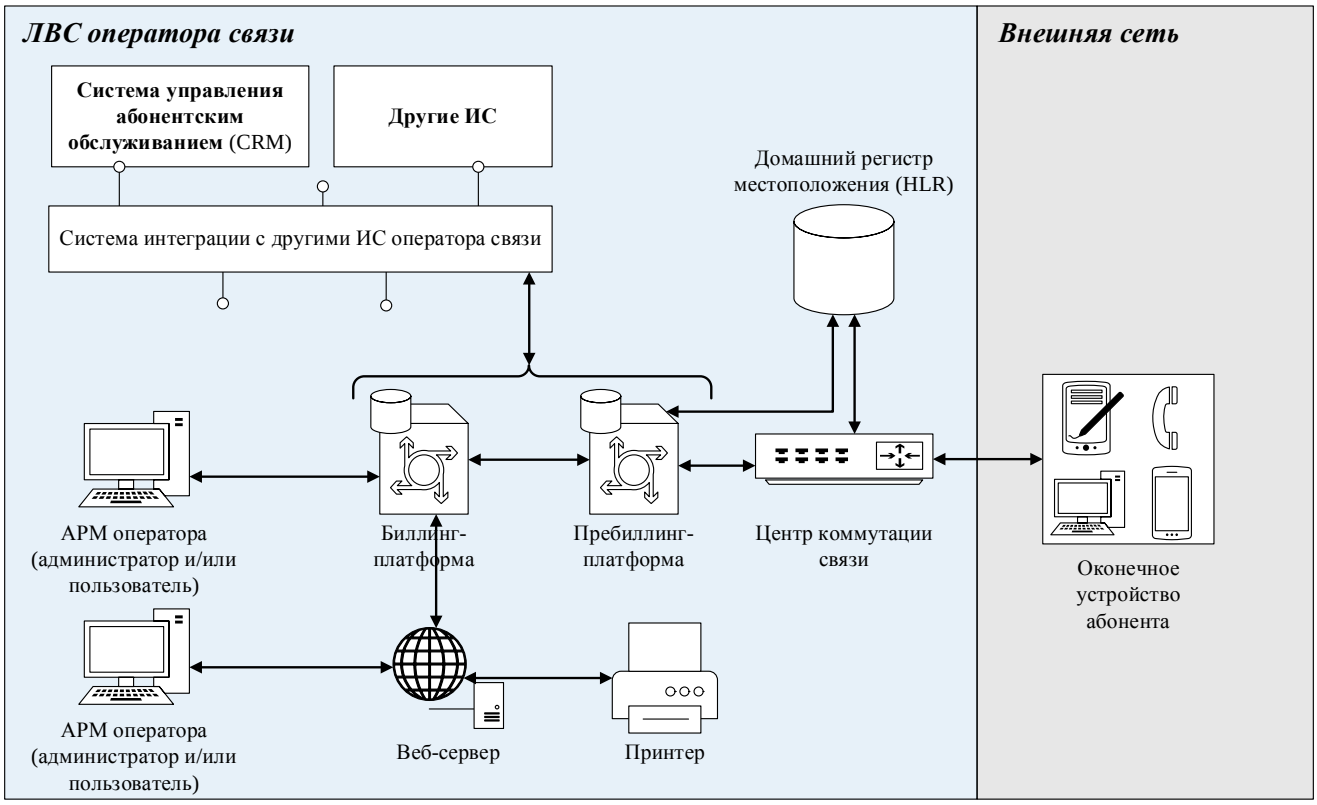

Рисунок 6 – Схема типовой автоматизированной системы расчетов

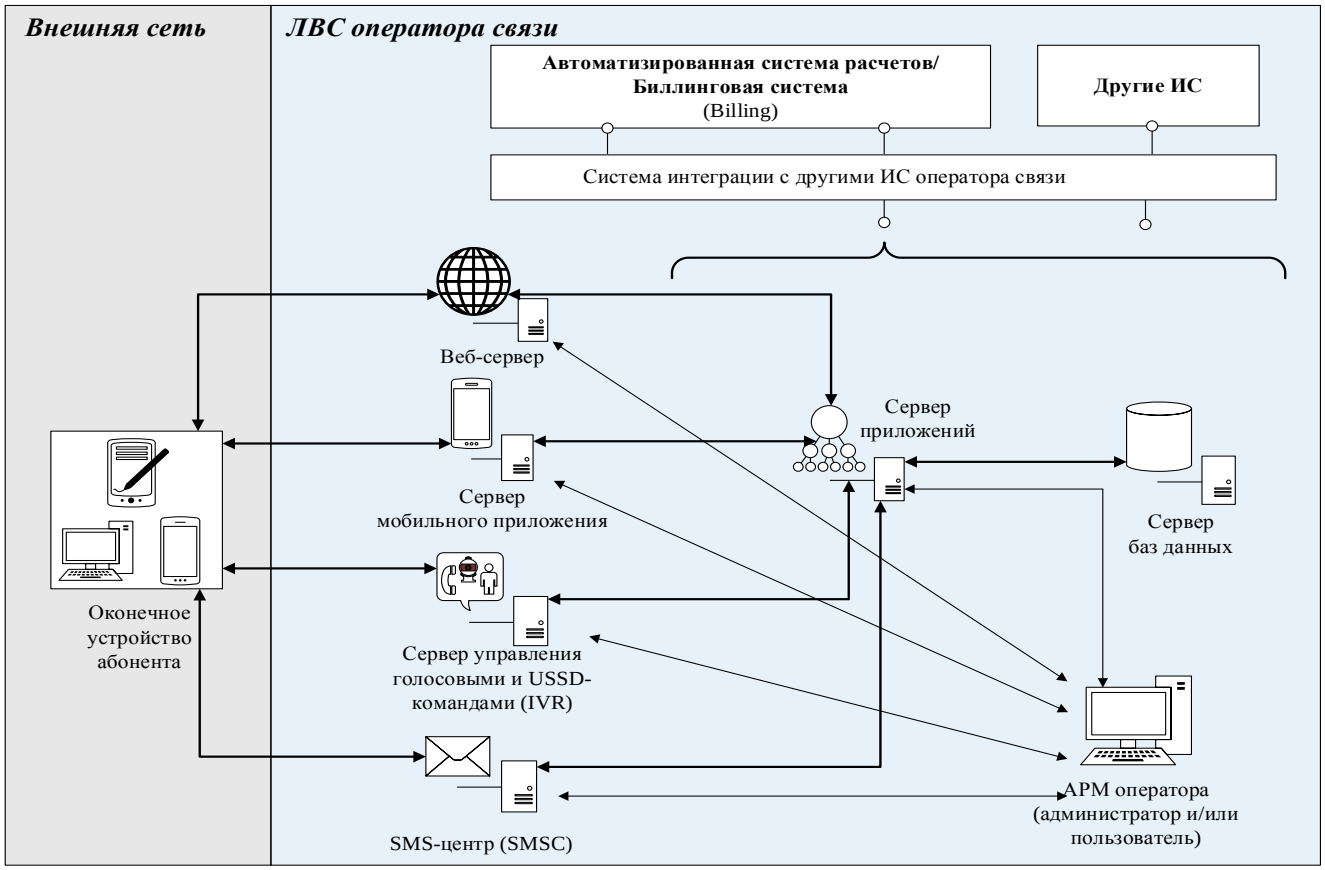

Рисунок 7 – Схема типовой системы самообслуживания абонентов

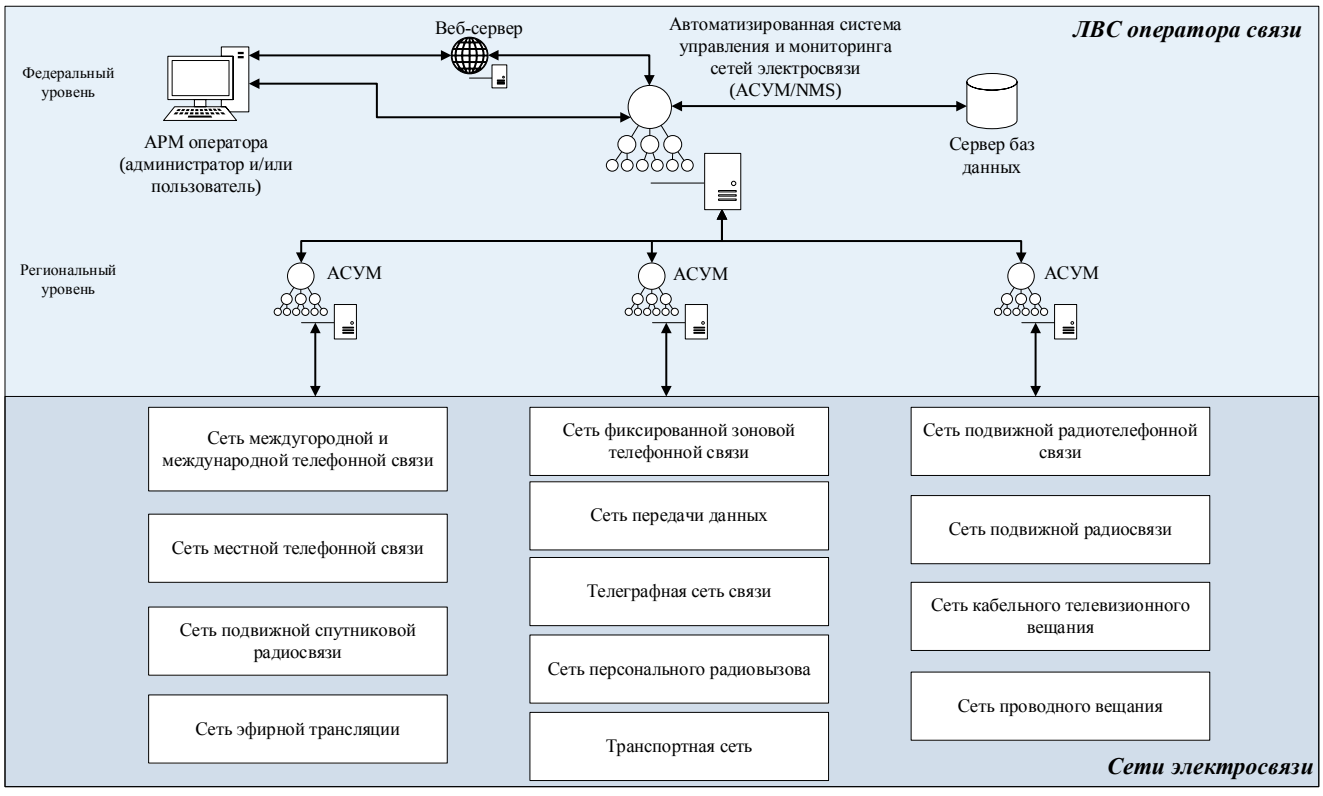

Рисунок 8 – Схема типовой автоматизированной системы управления и мониторинга сетей электросвязи

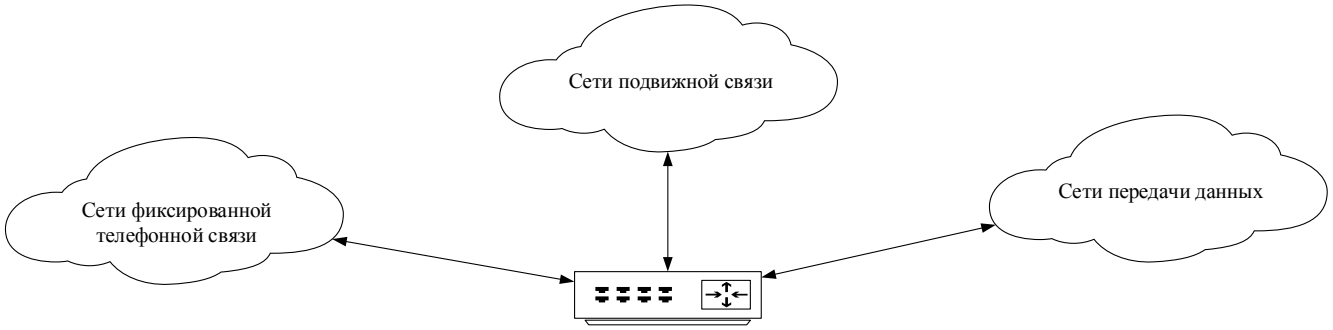

Рисунок 9 – Схема типового выделенного транзитного пункта сигнализации

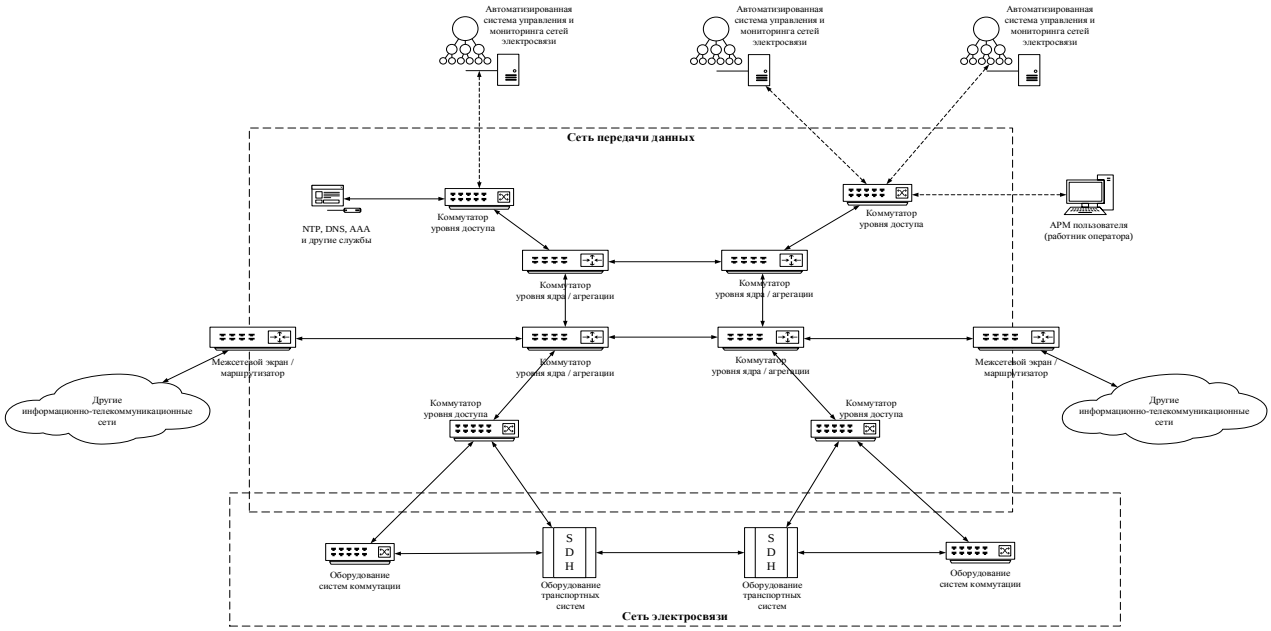

Рисунок 10 – Схема типовой выделенной сети передачи данных для управления и мониторинга сетей электросвязи

Приложение Д

Модель нарушителя в отношении типовых объектов критической информационной инфраструктуры, принадлежащих операторам связи

Принимая во внимание, что в соответствии с Федеральным законом N 187-ФЗ [2] обеспечение безопасности объектов КИИ направлено на обеспечение устойчивого функционирования объектов КИИ при проведении в отношении них компьютерных атак, в качестве источников угроз безопасности информации будут рассматриваться лица, преднамеренно совершающие действия, следствием которых является нарушение и/или прекращение функционирования сети связи (далее – нарушители).

Моделирование нарушителей безопасности информации в отношении объектов КИИ предназначено для формирования предположения о типах нарушителей, а также об основных возможностях нарушителей по реализации угроз безопасности информации в отношении типовых объектов КИИ в части оснащенности, знаний нарушителей (компетенции и знаний об объектах КИИ) и мотивации (целей).

Типы нарушителей

В зависимости от имеющихся прав физического (непосредственного) и/или логического доступа к компонентам типового объекта КИИ нарушители подразделяются на два типа (категории):

– внешние нарушители – лица, не имеющие прав доступа к компонентам типового объекта КИИ и реализующие угрозы безопасности информации из-за границ типового объекта КИИ;

– внутренние нарушители – лица, имеющие права постоянного или разового доступа к компонентам типового объекта КИИ и реализующие угрозы безопасности информации, находясь как внутри, так и вне границ типового объекта КИИ.

Мотивация (цели) нарушителей

С учетом положений ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения» [28] в качестве возможной мотивации (целей) реализации нарушителями угроз безопасности информации могут быть:

– нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;

– дискредитация или дестабилизация деятельности органов государственной власти, операторов связи;

– совершение террористических актов;

– идеологические или политические мотивы;

– причинение имущественного ущерба;

– продажа выявленных уязвимостей и получение финансовой выгоды;

– получение конкурентных преимуществ;

– любопытство или желание самореализации (подтверждение статуса);

– месть.

Оснащенность нарушителей

В зависимости от доступных нарушителю программных и/или программно-аппаратных средств, предназначенных для идентификации и использования уязвимостей компонентов объекта КИИ для реализации угроз безопасности информации, оснащенность нарушителя может быть следующая:

1. *Стандартные средства*. Легко доступные программные (программно-аппаратные) средства, к которым относятся:

– программные средства типового объекта КИИ, доступные внутренним нарушителям в соответствии с имеющимися правами доступа (например, встроенные средства операционной системы: отладчик, средства разработки и иные);

– программные средства, имеющиеся в свободном доступе (на бесплатной или платной основе) в общедоступных источниках, в том числе в сети Интернет (например, анализаторы протоколов).

2. *Специализированные средства*, отсутствующие в свободном доступе, но которые могут быть приобретены нарушителем без значительных усилий:

– программные (программно-аппаратные) средства, которые имеются в продаже (например: анализаторы кода; вредоносное ПО; компьютеры, объединенные через сеть Интернет (бот-сети));

– программные (программно-аппаратные) средства, разрабатываемые нарушителем.

3. *Средства, сделанные на заказ*, недоступные широкому кругу лиц, так как требуется их специальная разработка с привлечением исследовательских организаций, или распространение которых контролируется в соответствии с законодательством, а также дорогостоящие средства или средства, сведения о которых относятся к информации ограниченного доступа.

Знания нарушителей

Компетентность нарушителя в зависимости от его уровня знаний и подготовки в области информационных технологий и защиты информации может быть следующая:

1. *Непрофессионал*. Нарушитель имеет слабую осведомленность (по сравнению со специалистами или профессионалами) о мерах защиты информации, применяемых в отношении объектов КИИ данного типа, и не обладает специальными знаниями по реализации угроз безопасности информации.

2. *Специалист*. Нарушитель имеет осведомленность о мерах защиты информации, применяемых в отношении объектов КИИ данного типа.

3. *Профессионал*. Нарушитель имеет хорошую осведомленность о мерах защиты информации, применяемых в отношении объектов КИИ данного типа, об алгоритмах, аппаратных и программных средствах объектов КИИ данного типа, а также обладает специальными знаниями о методах и средствах выявления новых уязвимостей и способах реализации угроз безопасности информации в отношении объектов КИИ данного типа.

В зависимости от сведений о конкретном объекте КИИ и условиях его эксплуатации, доступных нарушителю, чтобы идентифицировать и использовать уязвимости для реализации угрозы безопасности информации, знания нарушителя о конкретном объекте КИИ могут быть следующие:

1. *Отсутствие знаний*. Нарушитель не обладает информацией о структурно-функциональных характеристиках объекта КИИ, его системе безопасности, а также об иной информации по разработке (проектированию) и эксплуатации конкретного объекта КИИ, включая сведения из конструкторской, проектной и эксплуатационной документации[35]. При этом нарушителю может быть доступна информация о целях и задачах, решаемых объектом КИИ.

2. *Ограниченные знания*. Нарушителю известны:

– информация о целях и задачах, решаемых объектом КИИ;

– фрагменты информации о топологии сети объекта КИИ;

– фрагменты информации о системном и/или прикладном ПО объекта КИИ;

– эксплуатационная документация на объект КИИ (в частности руководство пользователя и/или правила эксплуатации объекта КИИ).

3. *Знание чувствительной информации*. Нарушителю известны:

– конструкторская (проектная) и эксплуатационная документация на объект КИИ;

– информация о структурно-функциональных характеристиках объекта КИИ, в том числе полная информация о системном и/или прикладном ПО, технических средствах и конфигурации сети;

– информация о системе безопасности объекта КИИ.

Актуальные нарушители

В качестве актуальных нарушителей рассматриваются внешние и внутренние нарушители, оснащенные в т.ч. средствами, сделанными на заказ, с компетенцией профессионалов, со знанием чувствительной информации и с достаточной мотивацией для реализации угроз без-

[35] Знания о типовых объектах КИИ не рассматриваются как знания о конкретном объекте КИИ.

опасности информации, которые могут привести к нарушению и/или прекращению функционирования сети связи.

Приложение Е

Перечень основных угроз безопасности информации в отношении типовых объектов критической информационной инфраструктуры, принадлежащих операторам связи

В отношении типовых объектов КИИ, принадлежащих операторам связи, актуальны следующие основные типы угроз безопасности информации:

1. Угрозы создания нештатных режимов работы.
2. Угрозы доступа (проникновения) в операционную среду.

2.1. Угрозы непосредственного доступа.

2.1.1. Угрозы, реализуемые в ходе загрузки ОС.

2.1.2. Угрозы, реализуемые после загрузки ОС, независимо от того, какая программа запускается пользователем.

2.1.3. Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ.

2.2. Угрозы удаленного доступа (сетевые атаки).

2.2.1. Анализ сетевого трафика.

2.2.2. Сканирование сети.

2.2.3. «Парольная» атака.

2.2.4. Подмена доверенного объекта сети.

2.2.5. Навязывание ложного маршрута.

2.2.6. Внедрение ложного объекта сети.

2.2.7. Отказ в обслуживании.

2.2.8. Удаленный запуск приложений.

3. Угрозы программно-математического воздействия.

Данный перечень сформирован с использованием Базовой модели угроз безопасности информации [29] и рекомендуется для заполнения пункта 6.2 Формы направления сведений о результатах категорирования [27].

Приложение Ж

Обоснование неприменимости ряда показателей критериев значимости для типовых объектов критической информационной инфраструктуры, принадлежащих операторам связи

Таблица 15 – Обоснование неприменимости ряда показателей критериев значимости

№	Формулировка показателя	Обоснование неприменимости
I. Социальная значимость		
1.	Причинение ущерба жизни и здоровью людей (человек)	Объект КИИ не управляет процессами, связанными с причинением ущерба для жизни и здоровья людей
2.	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений	Объект КИИ не управляет объектами обеспечения жизнедеятельности населения
3.	Прекращение или нарушение функционирования объектов транспортной инфраструктуры	Объект КИИ не управляет объектами транспортной инфраструктуры
5.	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	Объект КИИ единолично не обеспечивает доступ к государственной услуге (оператор связи не имеет государственного задания (заказа) или муниципального задания (заказа) на оказание государственной услуги)
II. Политическая значимость		
6.	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	Оператор связи не имеет соответствующего действующего государственного контракта на оказание услуг связи государственному органу (оператор связи не является государственным органом)
7.	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации	Объект КИИ не обеспечивает соблюдение условий международного договора Российской Федерации (оператор связи не нарушает условия международных договоров Российской Федерации)
III. Экономическая значимость		
8.	Возникновение ущерба субъекту кри-	Оператор связи не является государственной

№	Формулировка показателя	Обоснование неприменимости
	тической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)	корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием
10.	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов – на основе прогнозных значений)	Объект КИИ единолично не обеспечивает проведение банковских операций (оператор связи не является системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка)
IV. Экологическая значимость		
11.	Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, по-	Объект КИИ не управляет объектами, способными оказывать негативное воздействие на окружающую среду

№	Формулировка показателя	Обоснование неприменимости
	вышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия)	
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка		
12.	Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра	Объект КИИ не участвует в функционировании пункта управления (ситуационного центра)
13.	Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры	Объект КИИ не участвует в обеспечении показателя государственного оборонного заказа
14.	Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)	Объект КИИ не участвует в функционировании информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка

Приложение И

Рекомендуемая форма акта по итогам категорирования объекта критической информационной инфраструктуры, принадлежащего оператору связи

Утвержден
приказом № Х от ДД.ММ.ГГГГ

АКТ
категорирования объекта критической информационной инфраструктуры

Комиссией по категорированию объектов критической информационной инфраструктуры, принадлежащих *название оператора связи* на праве собственности, аренды или ином законном основании и перечисленных в перечне объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию, утвержденном *ДД.ММ.ГГГГ, должность*,

ПРИНЯТО РЕШЕНИЕ [*выбрать один из двух вариантов*]:

- Присвоить объекту критической информационной инфраструктуры «*наименование объекта КИИ*» *Х* категорию значимости.
- Отсутствует необходимость присвоения одной из категорий значимости объекту критической информационной инфраструктуры «*наименование объекта КИИ*».

Сведения об объекте критической информационной инфраструктуры, результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, реализованные меры по обеспечению безопасности объекта критической информационной инфраструктуры, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, приведены в приложении (Приложение 1).

Приложение № 1 к акту
категорирования объектов критической информационной инфраструктуры

Сведения об объекте критической информационной инфраструктуры, результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, реализованные меры по обеспечению безопасности объекта критической информационной инфраструктуры, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры

по форме из приложения И

Приложение К

Рекомендации по заполнению содержательной части формы направления сведений о результатах категорирования для типовых объектов критической информационной инфраструктуры, принадлежащих операторам связи[36]

Условные обозначения, используемые в таблицах ниже (см. Таблица 16 – Таблица 20):

текст – сведения, которые не должны быть заменены оператором связи.

текст – сведения, которые должны быть заменены оператором связи на реальные.

[*текст*] – сведения, не подлежащие отражению в заполненной оператором связи форме (комментарий для заполняющего лица).

< *текст* > *или* < *текст* > – сведения, требующие выбора оператором связи из предложенных вариантов (неприменимые варианты удаляются оператором связи).

Таблица 16 – Сведения о результатах категорирования Автоматизированной системы расчетов «*Наименование*»

№	Параметр	Сведения
1.	Сведения об объекте критической информационной инфраструктуры	
1.1.	Наименование объекта	Автоматизированная система расчетов «*Наименование*»
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	*Подразделение / филиал / представительство: Адрес:* – *название улицы, номер дома;* – *название населенного пункта (города, поселка и т.п.);* – *название района;* – *название республики, края, области, автономного округа (области);* – *почтовый индекс* Сегментов нет [*указываются в случае наличия вместе с адресами размещения*]
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	Связь
1.4.	Назначение объекта	1. Автоматизация расчетов с абонентами за любые виды оказываемых им или заказываемых ими услуг связи в любом сочетании за исключе-

[36] Утверждается руководителем оператора связи или уполномоченным им лицом.
При необходимости проставляется ограничительная пометка или гриф секретности.

№	Параметр	Сведения
		нием услуг связи, оказываемых с использованием таксофонов, услуг телеграфной связи и услуг почтовой связи. 2. Автоматизация предобработки информации об оказанных услугах связи (пребиллинг). 3. Автоматизация задач активации продуктов и услуг связи. 4. Информационное обеспечение работников оператора связи сведениями для предоставления абоненту информации об оказанных услугах связи по запросу (в т.ч. выдача на твердую копию). 5. Информационное обеспечение работников оператора связи в рамках проведения взаиморасчетов между операторами связи. 6. Хранение данных о состоянии счетов абонентов. 7. Автоматизация задач предоставления услуг связи (в т.ч. ограничения предоставления услуг связи) для предоплатной модели расчетов («prepaid») [*указывается в случае наличия и использования данного функционала*]
1.5.	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	Управление и эксплуатация услуг (SM&O)
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	Клиент-серверная система, технология «тонкий клиент» [*указывается в случае наличия технологии «тонкий клиент»*]
2.	Сведения о субъекте критической информационной инфраструктуры	
2.1.	Наименование субъекта	*Наименование оператора связи*
2.2.	Адрес местонахождения субъекта	*Адрес места государственной регистрации оператора связи:* – *название улицы, номер дома;* – *название населенного пункта (города, поселка и т.п.);* – *название района;* – *название республики, края, области, автономного округа (области);* – *почтовый индекс*
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	*Должность, фамилия, имя, отчество*
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых	*Должность, фамилия, имя, отчество*

№	Параметр	Сведения
	объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	*Наименование структурного подразделения* [*указывается в случае наличия данного подразделения*], *Должность руководителя подразделения* [*указывается в случае наличия данного подразделения*] *или штатного специалиста,* *фамилия, имя, отчество,* *телефон,* *адрес электронной почты*
3.	Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи	
3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Общего пользования [*указываются иные категории сетей электросвязи в случае наличия взаимодействия*]
3.2.	Наименование оператора связи	*Наименование оператора связи* [*это сам оператор связи, т.к. с его сетью электросвязи взаимодействует объект КИИ*]
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Контроль/мониторинг технологического оборудования (оборудование сети электросвязи), оказание услуг связи, управление [*указываются в случае наличия и использования данного функционала*]
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	Тип доступа: Проводной, беспроводной. Технология доступа: xDSL, FE, P2P fiber. Протокол взаимодействия: протоколы стека TCP/IP [*может быть уточнено по решению оператора связи*]
4.	Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры	
4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	[*Ввести сквозную нумерацию эксплуатантов*] *1. Наименование оператора связи* [*если оператор связи сам эксплуатирует объект КИИ*] *2. Название юридического лица* [*если оно эксплуатирует объект КИИ*]. *3. Фамилия, имя, отчество индивидуального предпринимателя* [*если он эксплуатирует объект КИИ*]

№	Параметр	Сведения
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	[*Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*] *1. Адрес:* *– название улицы, номер дома;* *– название населенного пункта (города, поселка и т.п.);* *– название района;* *– название республики, края, области, автономного округа (области);* *– почтовый индекс* *2. Адрес: …*
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	[*Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*] *1. Элементы:* *< Биллинг-платформа >* *< Пребиллинг-платформа >* *< Веб-сервер >* *< АРМ пользователя >* *< иные компоненты >* [*указываются в случае наличия*] *2. Элементы: …*
5.	Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры	
5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	*Наименования программно-аппаратных средств и их количество (шт.)*
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	*Наименования общесистемного программного обеспечения*
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	*Наименования прикладных программ*
5.4.	Применяемые средства защиты информации (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки; функции безопасности программного обеспечения, если в него встроены средства защиты информации (идентификация, аутентификация,	*Наименования средств защиты информации* (*< номер и дата выдачи сертификата(ов) соответствия > или < номер и дата документа, содержащего результаты оценки соответствия > или < оценка соответствия не проводилась >*) [*указывается на каждое средство*] Функции идентификации и аутентификации, управления доступом, регистрации событий, резервного копирования, отказоустойчивости,

№	Параметр	Сведения
	управление доступом, регистрация событий безопасности, фильтрация, иные функции) или сведения об отсутствии средств защиты информации.	обеспечения целостности обрабатываемой информации в соответствие с Правилами применения автоматизированных систем расчетов, утв. приказом Министерства информационных технологий и связи Российской Федерации от 02.07.2007 N 73. *иные функции* [*указываются в случае наличия*]
6.	Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры	
6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	Внешние и внутренние нарушители, оснащенные в т.ч. средствами, сделанными на заказ, с компетенцией профессионалов, со знанием чувствительной информации и с достаточной мотивацией для реализации угроз безопасности информации согласно «Методическим рекомендациям по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи» (шифр: «КИИ-С-ССОП»)
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	1. Угрозы создания нештатных режимов работы. 2. Угрозы доступа (проникновения) в операционную среду. 2.1. Угрозы непосредственного доступа. 2.1.1. Угрозы, реализуемые в ходе загрузки ОС. 2.1.2. Угрозы, реализуемые после загрузки ОС, независимо от того, какая программа запускается пользователем. 2.1.3. Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. 2.2. Угрозы удаленного доступа (сетевые атаки). 2.2.1. Анализ сетевого трафика. 2.2.2. Сканирование сети. 2.2.3. «Парольная» атака. 2.2.4. Подмена доверенного объекта сети. 2.2.5. Навязывание ложного маршрута. 2.2.6. Внедрение ложного объекта сети. 2.2.7. Отказ в обслуживании. 2.2.8. Удаленный запуск приложений. 3. Угрозы программно-математического воздействия Реализация угроз < *может привести* > *или* < *не может привести* > к прекращению или нарушению функционирования сети связи
7.	Возможные последствия в случае возникновения компьютерных инцидентов	
7.1.	Типы компьютерных инцидентов, которые мо-	1. Отказ в обслуживании.

№	Параметр	Сведения
	гут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	2. Несанкционированный доступ. 3. Утечка данных (нарушение конфиденциальности). 4. Модификация (подмена) данных. 5. Нарушение функционирования технических средств. 6. Несанкционированное использование вычислительных ресурсов объекта Возникающие инциденты < *могут привести* > *или* < *не могут привести* > к прекращению или нарушению функционирования сети связи
7.2.	Ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" или обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов	Социальный «Прекращение или нарушение функционирования сети связи» (*количество абонентов, зона обслуживания*). Политический «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» (*наименование органа(ов) государственной власти, указывается в случае наличия соответствующего действующего государственного контракта*). Экономический «Возникновение ущерба бюджетам Российской Федерации» (*значения потенциально возможных ущербов бюджетам, тыс. рублей и процент*) < *Экологический* > *или* < *Для обороны страны, безопасности государства и правопорядка* > *с соответствующими показателями и значениями* [*если рассмотрены соответствующие виды негативных последствий*]
8.	Категория значимости, которая присвоена объекту критической информационной инфраструктуры	
8.1.	Категория значимости, которая присвоена объекту	< *I категория* > < *II категория* > < *III категория* > < *Отсутствует необходимость присвоения одной из категорий значимости* >
8.2.	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	4. а) Территория, на которой возможно прекращение или нарушение функционирования сети связи: *указать наименование субъекта(ов) РФ (зону обслуживания данным объектом КИИ).* 4. б) Количество людей, для которых могут быть недоступны услуги связи: *указать количество абонентов (тысяч).* 6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия): *указать наименование органа(ов) государственной власти* (*указывается в случае наличия соответствующего действующего государственного контракта).*

№	Параметр	Сведения
		9. а) Снижение доходов федерального бюджета: *указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах.* 9. б) Снижение доходов бюджета субъекта РФ: *указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах* [*указываются последовательно для всех субъектов РФ, входящих в зону обслуживания данным объектом КИИ*] 9. в) Не возникает снижение доходов бюджетов государственных внебюджетных фондов вследствие компьютерных атак на объект КИИ [*Информация о неприменимости остальных показателей приведена в приложении Ж, требуется ее сюда скопировать, в случае их неприменимости; если показатель применим, то требуется указать и показатель, и полученное по нему значение*]
9.	Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры	
9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	Установлена контролируемая зона. Обеспечен контроль физического доступа к объекту КИИ. Разработаны документы (регламенты, инструкции, руководства): – *Название и реквизиты документа;* – *Название и реквизиты документа* *Иные меры* [*указываются в случае наличия*]
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	Меры по идентификации и аутентификации, управлению доступом, регистрации событий, резервному копированию, отказоустойчивости, обеспечению целостности обрабатываемой информации выполнены в соответствие с Правилами применения автоматизированных систем расчетов, утв. приказом Министерства информационных технологий и связи Российской Федерации от 02.07.2007 N 73. *Меры:* – *идентификация и аутентификация (ИАФ);* – *управление доступом (УПД);* – *ограничение программной среды (ОПС);* – *защита машинных носителей информации (ЗНИ);* – *аудит безопасности (АУД);* – *антивирусная защита (АВЗ);* – *предотвращение вторжений (компьютерных атак) (СОВ);* – *обеспечение целостности (ОЦЛ);* – *обеспечение доступности (ОДТ);* – *защита технических средств и систем (ЗТС);*

№	Параметр	Сведения
		– защита информационной (автоматизированной) системы и ее компонентов (ЗИС).

Таблица 17 – Сведения о результатах категорирования Системы самообслуживания абонентов «*Наименование*»

№	Параметр	Сведения
1.	Сведения об объекте критической информационной инфраструктуры	
1.1.	Наименование объекта	Система самообслуживания абонентов «*Наименование*»
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	*Подразделение / филиал / представительство: Адрес:* *– название улицы, номер дома;* *– название населенного пункта (города, поселка и т.п.);* *– название района;* *– название республики, края, области, автономного округа (области);* *почтовый индекс* Сегментов нет [*указываются в случае наличия вместе с адресами размещения*]
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	Связь
1.4.	Назначение объекта	1. Автоматизация задач управления набором услуг, предоставляемых абонентам. 2. Автоматизация задач подключения/отключения дополнительных услуг, смены тарифного плана абонентом. 3. Информационное обеспечение абонента справочными сведениями, в т.ч. о состоянии его лицевого счета (баланса)
1.5.	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	Управление и эксплуатация услуг (SM&O)
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	Клиент-серверная система, технология «тонкий клиент» [*указывается в случае наличия технологии «тонкий клиент»*]

№	Параметр	Сведения
2.	Сведения о субъекте критической информационной инфраструктуры	
2.1.	Наименование субъекта	*Название оператора связи*
2.2.	Адрес местонахождения субъекта	*Адрес места государственной регистрации оператора связи:* *– название улицы, номер дома;* *– название населенного пункта (города, поселка и т.п.);* *– название района;* *– название республики, края, области, автономного округа (области);* *– почтовый индекс*
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	*Должность, фамилия, имя, отчество*
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	*Должность, фамилия, имя, отчество*
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	*Наименование структурного подразделения* [*указывается в случае наличия данного подразделения*], *Должность руководителя подразделения* [*указывается в случае наличия данного подразделения*] *или штатного специалиста,* *фамилия, имя, отчество,* *телефон,* *адрес электронной почты*
3.	Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи	
3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Общего пользования [*указываются иные категории сетей электросвязи в случае наличия взаимодействия*]
3.2.	Наименование оператора связи	*Наименование оператора связи* [*это сам оператор связи, т.к. с его сетью электросвязи взаимодействует объект КИИ*]
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнитель-	Управление (включение/отключение услуг связи), оказание услуг

№	Параметр	Сведения
	ными устройствами), иная цель)	
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	Тип доступа: Проводной, беспроводной. Технология доступа: xDSL, GPON. Протокол взаимодействия: протоколы стека TCP/IP [*может быть уточнено по решению оператора связи*]
4.	Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры	
4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	[*Ввести сквозную нумерацию эксплуатантов*] *1. Наименование оператора связи* [*если оператор связи сам эксплуатирует объект КИИ*] *2. Название юридического лица* [*если оно эксплуатирует объект КИИ*]. *3. Фамилия, имя, отчество индивидуального предпринимателя* [*если он эксплуатирует объект КИИ*]
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	[*Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*] *1. Адрес:* *– название улицы, номер дома;* *– название населенного пункта (города, поселка и т.п.);* *– название района;* *– название республики, края, области, автономного округа (области);* *– почтовый индекс* *2. Адрес: …*
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	[*Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*] *1. Элементы:* *< Сервер приложений >* *< Сервер баз данных >* *< Веб-сервер >* *< Сервер мобильного приложения >* *< Сервер управления голосовыми и USSD-командами (IVR) >* *< SMS-центр >* *< иные компоненты >* [*указываются в случае наличия*] *2. Элементы: …*
5.	Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры	
5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, про-	*Наименования программно-аппаратных средств и их количество (шт.)*

№	Параметр	Сведения
	изводственного оборудования (исполнительных устройств), иных средств) и их количество	
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	*Наименования общесистемного программного обеспечения*
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	*Наименования прикладных программ*
5.4.	Применяемые средства защиты информации (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки; функции безопасности программного обеспечения, если в него встроены средства защиты информации (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции) или сведения об отсутствии средств защиты информации.	*Наименования средств защиты информации* (< *номер и дата выдачи сертификата(ов) соответствия* > *или* < *номер и дата документа, содержащего результаты оценки соответствия* > *или* < *оценка соответствия не проводилась* >) [*указывается на каждое средство*] *идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции* [*указываются в случае наличия*]
6.	Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры	
6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	Внешние и внутренние нарушители, оснащенные в т.ч. средствами, сделанными на заказ, с компетенцией профессионалов, со знанием чувствительной информации и с достаточной мотивацией для реализации угроз безопасности информации согласно «Методическим рекомендациям по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи» (шифр: «КИИ-С-ССОП»)
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	1. Угрозы создания нештатных режимов работы. 2. Угрозы доступа (проникновения) в операционную среду. 2.1. Угрозы непосредственного доступа. 2.1.1. Угрозы, реализуемые в ходе загрузки ОС. 2.1.2. Угрозы, реализуемые после загрузки ОС, независимо от того, какая программа запускается пользователем. 2.1.3. Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ.

№	Параметр	Сведения
		2.2. Угрозы удаленного доступа (сетевые атаки). 2.2.1. Анализ сетевого трафика. 2.2.2. Сканирование сети. 2.2.3. «Парольная» атака. 2.2.4. Подмена доверенного объекта сети. 2.2.5. Навязывание ложного маршрута. 2.2.6. Внедрение ложного объекта сети. 2.2.7. Отказ в обслуживании. 2.2.8. Удаленный запуск приложений. 3. Угрозы программно-математического воздействия Реализация угроз < *может привести* > *или* < *не может привести* > к прекращению или нарушению функционирования сети связи
7.	Возможные последствия в случае возникновения компьютерных инцидентов	
7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	1. Отказ в обслуживании. 2. Несанкционированный доступ. 3. Утечка данных (нарушение конфиденциальности). 4. Модификация (подмена) данных. 5. Нарушение функционирования технических средств. 6. Несанкционированное использование вычислительных ресурсов объекта Возникающие инциденты < *могут привести* > *или* < *не могут привести* > к прекращению или нарушению функционирования сети связи
7.2.	Ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" или обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов	Социальный «Прекращение или нарушение функционирования сети связи» (*количество абонентов, зона обслуживания*). Политический «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» (*наименование органа(ов) государственной власти, указывается в случае наличия соответствующего действующего государственного контракта*). Экономический «Возникновение ущерба бюджетам Российской Федерации» (*значения потенциально возможных ущербов бюджетам, тыс. рублей и процент*) < *Экологический* > *или* < *Для обороны страны, безопасности государства и правопорядка* > *с соответствующими показателями и значениями* [*если рассмотрены соответствующие виды негативных последствий*]
8.	Категория значимости, которая присвоена объекту критической информационной инфраструктуры	
8.1.	Категория значимости, которая присвоена объекту	< *I категория* > < *II категория* >

№	Параметр	Сведения
		< III категория > *< Отсутствует необходимость присвоения одной из категорий значимости >*
8.2.	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	4. а) Территория, на которой возможно прекращение или нарушение функционирования сети связи: *указать наименование субъекта(ов) РФ (зону обслуживания данным объектом КИИ).* 4. б) Количество людей, для которых могут быть недоступны услуги связи: *указать количество абонентов (тысяч).* 6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия): *указать наименование органа(ов) государственной власти (указывается в случае наличия соответствующего действующего государственного контракта).* 9. а) Снижение доходов федерального бюджета*: указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах.* 9. б) Снижение доходов бюджета субъекта РФ: *указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах* [*указываются последовательно для всех субъектов РФ, входящих в зону обслуживания данным объектом КИИ*] 9. в) Не возникает снижение доходов бюджетов государственных внебюджетных фондов вследствие компьютерных атак на объект КИИ [*Информация о неприменимости остальных показателей приведена в приложении Ж, требуется ее сюда скопировать, в случае их неприменимости; если показатель применим, то требуется указать и показатель, и полученное по нему значение*]
9.	Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры	
9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	Установлена контролируемая зона. Обеспечен контроль физического доступа к объекту КИИ. Разработаны документы (регламенты, инструкции, руководства): – *Название и реквизиты документа;* – *Название и реквизиты документа* *Иные меры* [*указываются в случае наличия*]
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспе-	*Меры:* – *идентификация и аутентификация (ИАФ);* – *управление доступом (УПД);* – *ограничение программной среды (ОПС);*

№	Параметр	Сведения
	чению безопасности значимых объектов	– *защита машинных носителей информации (ЗНИ);* – *аудит безопасности (АУД);* – *антивирусная защита (АВЗ);* – *предотвращение вторжений (компьютерных атак) (СОВ);* – *обеспечение целостности (ОЦЛ);* – *обеспечение доступности (ОДТ);* – *защита технических средств и систем (ЗТС);* – *защита информационной (автоматизированной) системы и ее компонентов (ЗИС).*

Таблица 18 – Сведения о результатах категорирования Автоматизированной системы управления и мониторинга сетей электросвязи «*Наименование*»

№	Параметр	Сведения
1.	Сведения об объекте критической информационной инфраструктуры	
1.1.	Наименование объекта	Автоматизированная система управления и мониторинга сетей электросвязи «*Наименование*»
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	*Подразделение / филиал / представительство:* *Адрес:* – *название улицы, номер дома;* – *название населенного пункта (города, поселка и т.п.);* – *название района;* – *название республики, края, области, автономного округа (области);* – *почтовый индекс* Сегментов нет [*указываются в случае наличия вместе с адресами размещения*]
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	Связь
1.4.	Назначение объекта	1. Автоматизация и информационное обеспечение работников оператора связи в рамках задач управления неисправностями (инцидентами), контроль выполнения задач по устранению неисправностей. 2. Автоматизация и информационное обеспечение работников оператора связи в рамках задач мониторинга. 3. Автоматизация и информационное обеспечение работников оператора связи в рамках задач управления конфигурациями. 4. Автоматизация и информационное обеспече-

№	Параметр	Сведения
		ние работников оператора связи в рамках задач управления производительностью. 5. Автоматизация и информационное обеспечение работников оператора связи в рамках задач управления изменениями. 6. Автоматизация инвентаризации и технического учета
1.5.	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	1. Управление и эксплуатация услуг (SM&O). 2. Управление и эксплуатация ресурсов (RM&O)
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	Распределенная система управления, технология «тонкий клиент» [*указывается в случае наличия технологии «тонкий клиент»*]
2.	Сведения о субъекте критической информационной инфраструктуры	
2.1.	Наименование субъекта	*Наименование оператора связи*
2.2.	Адрес местонахождения субъекта	*Адрес места государственной регистрации оператора связи:* *– название улицы, номер дома;* *– название населенного пункта (города, поселка и т.п.);* *– название района;* *– название республики, края, области, автономного округа (области);* *– почтовый индекс*
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	*Должность, фамилия, имя, отчество*
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	*Должность, фамилия, имя, отчество*
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	*Наименование структурного подразделения* [*указывается в случае наличия данного подразделения*], *Должность руководителя подразделения* [*указывается в случае наличия данного подразделения*] *или штатного специалиста,* *фамилия, имя, отчество,* *телефон,* *адрес электронной почты*

№	Параметр	Сведения
3.	Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи	
3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Общего пользования [*указываются иные категории сетей электросвязи в случае наличия взаимодействия*
3.2.	Наименование оператора связи	*Наименование оператора связи* [*это сам оператор связи, т.к. с его сетью электросвязи взаимодействует объект КИИ*]
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Управление, контроль/мониторинг технологического оборудования (оборудование сети электросвязи)
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	Тип доступа: Проводной, беспроводной. Технология доступа: xDSL, FE, P2P fiber. Протокол взаимодействия: протоколы стека TCP/IP [*может быть уточнено по решению оператора связи*]
4.	Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры	
4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	[*Ввести сквозную нумерацию эксплуатантов*] *1. Наименование оператора связи* [*если оператор связи сам эксплуатирует объект КИИ*] *2. Название юридического лица* [*если оно эксплуатирует объект КИИ*]. *3. Фамилия, имя, отчество индивидуального предпринимателя* [*если он эксплуатирует объект КИИ*]
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	[*Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*] *1. Адрес:* *– название улицы, номер дома;* *– название населенного пункта (города, поселка и т.п.);* *– название района;* *– название республики, края, области, автономного округа (области);* *– почтовый индекс* *2. Адрес: …*
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное	[*Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*]

№	Параметр	Сведения
	оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	*1. Элементы:* *< Сервер приложений >* *< Веб-сервер >* *< Сервер баз данных >* *< АРМ пользователя >* *< иные компоненты >* [*указываются в случае наличия*] *2. Элементы: ...*
5.	Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры	
5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	*Наименования программно-аппаратных средств и их количество (шт.)*
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	*Наименования общесистемного программного обеспечения*
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	*Наименования прикладных программ*
5.4.	Применяемые средства защиты информации (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки; функции безопасности программного обеспечения, если в него встроены средства защиты информации (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции) или сведения об отсутствии средств защиты информации.	*Наименования средств защиты информации* (*< номер и дата выдачи сертификата(ов) соответствия > или < номер и дата документа, содержащего результаты оценки соответствия > или < оценка соответствия не проводилась >*) [*указывается на каждое средство*] Функции идентификации и аутентификации, управлению доступом, регистрации событий, резервному копированию, отказоустойчивости в соответствие с Правилами применения оборудования автоматизированных систем управления и мониторинга средств связи, выполняющих функции систем коммутации каналов утв. приказом Министерства информационных технологий и связи Российской Федерации от 15.05.2007 N 55 и Правилами применения оборудования автоматизированных систем управления и мониторинга средств связи, выполняющих функции систем коммутации и маршрутизации пакетов информации утв. приказом Министерства информационных технологий и связи Российской Федерации от 12.01.2009 N 2 *иные функции* [*указываются в случае наличия*]

№	Параметр	Сведения
6.	Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры	
6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	Внешние и внутренние нарушители, оснащенные в т.ч. средствами, сделанными на заказ, с компетенцией профессионалов, со знанием чувствительной информации и с достаточной мотивацией для реализации угроз безопасности информации согласно «Методическим рекомендациям по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи» (шифр: «КИИ-С-ССОП»)
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	1. Угрозы создания нештатных режимов работы. 2. Угрозы доступа (проникновения) в операционную среду. 2.1. Угрозы непосредственного доступа. 2.1.1. Угрозы, реализуемые в ходе загрузки ОС. 2.1.2. Угрозы, реализуемые после загрузки ОС, независимо от того, какая программа запускается пользователем. 2.1.3. Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. 2.2. Угрозы удаленного доступа (сетевые атаки). 2.2.1. Анализ сетевого трафика. 2.2.2. Сканирование сети. 2.2.3. «Парольная» атака. 2.2.4. Подмена доверенного объекта сети. 2.2.5. Навязывание ложного маршрута. 2.2.6. Внедрение ложного объекта сети. 2.2.7. Отказ в обслуживании. 2.2.8. Удаленный запуск приложений. 3. Угрозы программно-математического воздействия Реализация угроз < *может привести* > *или* < *не может привести* > к прекращению или нарушению функционирования сети связи
7.	Возможные последствия в случае возникновения компьютерных инцидентов	
7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование	1. Отказ в обслуживании. 2. Несанкционированный доступ. 3. Утечка данных (нарушение конфиденциальности). 4. Модификация (подмена) данных. 5. Нарушение функционирования технических средств. 6. Несанкционированное использование вычислительных ресурсов объекта

№	Параметр	Сведения
	вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	Возникающие инциденты < *могут привести* > *или* < *не могут привести* > к прекращению или нарушению функционирования сети связи
7.2.	Ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" или обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов	Социальный «Прекращение или нарушение функционирования сети связи» (*количество абонентов, зона обслуживания*). Политический «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» (*наименование органа(ов) государственной власти, указывается в случае наличия соответствующего действующего государственного контракта*). Экономический «Возникновение ущерба бюджетам Российской Федерации» (*значения потенциально возможных ущербов бюджетам, тыс. рублей и процент*) < *Экологический* > *или* < *Для обороны страны, безопасности государства и правопорядка* > *с соответствующими показателями и значениями* [*если рассмотрены соответствующие виды негативных последствий*]
8.	Категория значимости, которая присвоена объекту критической информационной инфраструктуры	
8.1.	Категория значимости, которая присвоена объекту	< *I категория* > < *II категория* > < *III категория* > < *Отсутствует необходимость присвоения одной из категорий значимости* >
8.2.	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	4. а) Территория, на которой возможно прекращение или нарушение функционирования сети связи: *указать наименование субъекта(ов) РФ (зону обслуживания данным объектом КИИ).* 4. б) Количество людей, для которых могут быть недоступны услуги связи: *указать количество абонентов (тысяч).* 6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия): *указать наименование органа(ов) государственной власти* (*указывается в случае наличия соответствующего действующего государственного контракта).* 9. а) Снижение доходов федерального бюджета*: указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах.* 9. б) Снижение доходов бюджета субъекта РФ: *указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах* [*указываются последовательно для всех субъ-*

№	Параметр	Сведения
		ектов РФ, входящих в зону обслуживания данным объектом КИИ] 9. в) Не возникает снижение доходов бюджетов государственных внебюджетных фондов вследствие компьютерных атак на объект КИИ [*Информация о неприменимости остальных показателей приведена в приложении Ж, требуется ее сюда скопировать, в случае их неприменимости; если показатель применим, то требуется указать и показатель, и полученное по нему значение*]
9.	Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры	
9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	Установлена контролируемая зона. Обеспечен контроль физического доступа к объекту КИИ. Разработаны документы (регламенты, инструкции, руководства): – *Название и реквизиты документа;* – *Название и реквизиты документа* *Иные меры* [*указываются в случае наличия*]
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	Меры по идентификации и аутентификации, управлению доступом, регистрации событий, резервному копированию, отказоустойчивости выполнены в соответствие с Правилами применения оборудования автоматизированных систем управления и мониторинга средств связи, выполняющих функции систем коммутации каналов утв. приказом Министерства информационных технологий и связи Российской Федерации от 15.05.2007 N 55 и Правилами применения оборудования автоматизированных систем управления и мониторинга средств связи, выполняющих функции систем коммутации и маршрутизации пакетов информации утв. приказом Министерства информационных технологий и связи Российской Федерации от 12.01.2009 N 2. *Меры:* – *идентификация и аутентификация (ИАФ);* – *управление доступом (УПД);* – *ограничение программной среды (ОПС);* – *защита машинных носителей информации (ЗНИ);* – *аудит безопасности (АУД);* – *антивирусная защита (АВЗ);* – *предотвращение вторжений (компьютерных атак) (СОВ);* – *обеспечение целостности (ОЦЛ);* – *обеспечение доступности (ОДТ);*

№	Параметр	Сведения
		– *защита технических средств и систем (ЗТС);* – *защита информационной (автоматизированной) системы и ее компонентов (ЗИС).*

Таблица 19 – Сведения о результатах категорирования Выделенного транзитного пункта сигнализации «*Наименование*»

№	Параметр	Сведения
1.	Сведения об объекте критической информационной инфраструктуры	
1.1.	Наименование объекта	Выделенный транзитный пункт сигнализации «*Наименование*»
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	*Подразделение / филиал / представительство:* *Адрес:* – *название улицы, номер дома;* – *название населенного пункта (города, поселка и т.п.);* – *название района;* – *название республики, края, области, автономного округа (области);* – *почтовый индекс* Сегментов нет [*указываются в случае наличия вместе с адресами размещения*]
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	Связь
1.4.	Назначение объекта	1. Управление сетью сигнализации, обработка сообщений сигнализации. 2. Передача сигнального трафика, маршрутизация сигнальных сообщений. 3. Сбор статистики сигнальных сообщений. 4. Защита от несанкционированного доступа в сеть общеканальной сигнализации N 7 (ОКС N 7). 5. Учет сигнального трафика для взаиморасчетов между операторами связи
1.5.	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	Управление и эксплуатация услуг (SM&O)
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная	Иная архитектура (локальное размещенное законченное программно-аппаратное средство)

№	Параметр	Сведения
	система управления, иная архитектура)	
2.	Сведения о субъекте критической информационной инфраструктуры	
2.1.	Наименование субъекта	*Наименование оператора связи*
2.2.	Адрес местонахождения субъекта	*Адрес места государственной регистрации оператора связи:* *– название улицы, номер дома;* *– название населенного пункта (города, поселка и т.п.);* *– название района;* *– название республики, края, области, автономного округа (области);* *– почтовый индекс*
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	*Должность, фамилия, имя, отчество*
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	*Должность, фамилия, имя, отчество*
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	*Наименование структурного подразделения* [*указывается в случае наличия данного подразделения*], *Должность руководителя подразделения* [*указывается в случае наличия данного подразделения*] *или штатного специалиста,* *фамилия, имя, отчество,* *телефон,* *адрес электронной почты*
3.	Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи	
3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Общего пользования [*указываются иные категории сетей электросвязи в случае наличия взаимодействия*]
3.2.	Наименование оператора связи	*Наименование оператора связи* [*это сам оператор связи, т.к. с его сетью электросвязи взаимодействует объект КИИ*]
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг,	Управление, оказание услуг

№	Параметр	Сведения
	управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	Тип доступа: Проводной. Технология доступа: xDSL, FE, P2P fiber. Протокол взаимодействия: ОКС N 7, SIGTRAN, Diameter [*может быть уточнено по решению оператора связи*]
4.	Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры	
4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	[*Ввести сквозную нумерацию эксплуатантов*] *1. Наименование оператора связи* [*если оператор связи сам эксплуатирует объект КИИ*] *2. Название юридического лица* [*если оно эксплуатирует объект КИИ*]. *3. Фамилия, имя, отчество индивидуального предпринимателя* [*если он эксплуатирует объект КИИ*]
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	[*Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*] *1. Адрес:* *– название улицы, номер дома;* *– название населенного пункта (города, поселка и т.п.);* *– название района;* *– название республики, края, области, автономного округа (области);* *– почтовый индекс* *2. Адрес: …*
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	[*Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*] 1. Непосредственно выделенный транзитный пункт сигнализации. 2. …
5.	Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры	
5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	< Signalling Transfer Point (STP) > - _ шт. < Diameter Routing Agent (DRA) > - _ шт.
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	*< Signalling Transfer Point (STP) > версия ПО* *< Diameter Routing Agent (DRA) > версия ПО*

№	Параметр	Сведения
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	Не применимо (т.к. является законченным программно-аппаратным средством)
5.4.	Применяемые средства защиты информации (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки; функции безопасности программного обеспечения, если в него встроены средства защиты информации (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции) или сведения об отсутствии средств защиты информации.	*Наименования средств защиты информации* (< *номер и дата выдачи сертификата(ов) соответствия* > или < *номер и дата документа, содержащего результаты оценки соответствия* > или < *оценка соответствия не проводилась* >) [*указывается на каждое средство*] *Идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции* [*указываются в случае наличия*]
6.	Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры	
6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	Внешние и внутренние нарушители, оснащенные в т.ч. средствами, сделанными на заказ, с компетенцией профессионалов, со знанием чувствительной информации и с достаточной мотивацией для реализации угроз безопасности информации согласно «Методическим рекомендациям по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи» (шифр: «КИИ-С-ССОП»)
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	1. Угрозы создания нештатных режимов работы. 2. Угрозы доступа (проникновения) в операционную среду. 2.1. Угрозы непосредственного доступа. 2.1.1. Угрозы, реализуемые в ходе загрузки ОС. 2.1.2. Угрозы, реализуемые после загрузки ОС, независимо от того, какая программа запускается пользователем. 2.1.3. Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. 2.2. Угрозы удаленного доступа (сетевые атаки). 2.2.1. Анализ сетевого трафика. 2.2.2. Сканирование сети. 2.2.3. «Парольная» атака. 2.2.4. Подмена доверенного объекта сети. 2.2.5. Навязывание ложного маршрута.

№	Параметр	Сведения
		2.2.6. Внедрение ложного объекта сети. 2.2.7. Отказ в обслуживании. 2.2.8. Удаленный запуск приложений. 3. Угрозы программно-математического воздействия Реализация угроз < *может привести* > *или* < *не может привести* > к прекращению или нарушению функционирования сети связи
7.	Возможные последствия в случае возникновения компьютерных инцидентов	
7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	1. Отказ в обслуживании. 2. Несанкционированный доступ. 3. Утечка данных (нарушение конфиденциальности). 4. Модификация (подмена) данных. 5. Нарушение функционирования технических средств. 6. Несанкционированное использование вычислительных ресурсов объекта Возникающие инциденты < *могут привести* > *или* < *не могут привести* > к прекращению или нарушению функционирования сети связи
7.2.	Ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" или обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов	Социальный «Прекращение или нарушение функционирования сети связи» (*количество абонентов, зона обслуживания*). Политический «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» (*наименование органа(ов) государственной власти, указывается в случае наличия соответствующего действующего государственного контракта*). Экономический «Возникновение ущерба бюджетам Российской Федерации» (*значения потенциально возможных ущербов бюджетам, тыс. рублей и процент*) < *Экологический* > *или* < *Для обороны страны, безопасности государства и правопорядка* > *с соответствующими показателями и значениями* [*если рассмотрены соответствующие виды негативных последствий*]
8.	Категория значимости, которая присвоена объекту критической информационной инфраструктуры	
8.1.	Категория значимости, которая присвоена объекту	< *I категория* > < *II категория* > < *III категория* > < *Отсутствует необходимость присвоения одной из категорий значимости* >
8.2.	Полученные значения по каждому из показателей критериев значимости с обоснованием или	4. а) Территория, на которой возможно прекращение или нарушение функционирования сети

№	Параметр	Сведения
	информация о неприменимости показателя к объекту с соответствующим обоснованием	связи: *указать наименование субъекта(ов) РФ (зону обслуживания данным объектом КИИ).* 4. б) Количество людей, для которых могут быть недоступны услуги связи: *указать количество абонентов (тысяч).* 6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия): *указать наименование органа(ов) государственной власти (указывается в случае наличия соответствующего действующего государственного контракта).* 9. а) Снижение доходов федерального бюджета*: указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах.* 9. б) Снижение доходов бюджета субъекта РФ: *указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах* [*указываются последовательно для всех субъектов РФ, входящих в зону обслуживания данным объектом КИИ*] 9. в) Не возникает снижение доходов бюджетов государственных внебюджетных фондов вследствие компьютерных атак на объект КИИ [*Информация о неприменимости остальных показателей приведена в приложении Ж, требуется ее сюда скопировать, в случае их неприменимости; если показатель применим, то требуется указать и показатель, и полученное по нему значение*]
9.	Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры	
9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	Установлена контролируемая зона. Обеспечен контроль физического доступа к объекту КИИ. Разработаны документы (регламенты, инструкции, руководства): – *Название и реквизиты документа;* – *Название и реквизиты документа* *Иные меры* [*указываются в случае наличия*]
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	*Меры:* – *идентификация и аутентификация (ИАФ);* – *управление доступом (УПД);* – *ограничение программной среды (ОПС);* – *защита машинных носителей информации (ЗНИ);* – *аудит безопасности (АУД);* – *антивирусная защита (АВЗ);* – *предотвращение вторжений (компьютерных атак) (СОВ);*

№	Параметр	Сведения
		– *обеспечение целостности (ОЦЛ);* – *обеспечение доступности (ОДТ);* – *защита технических средств и систем (ЗТС);* – *защита информационной (автоматизированной) системы и ее компонентов (ЗИС).*

Таблица 20 – Сведения о результатах категорирования Выделенной сети передачи данных для управления и мониторинга сетей электросвязи «*Наименование*»

№	Параметр	Сведения
1.	Сведения об объекте критической информационной инфраструктуры	
1.1.	Наименование объекта	Выделенная сеть передачи данных для управления и мониторинга сетей электросвязи «*Наименование*»
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	*Подразделение / филиал / представительство:* *Адрес размещения core-компонентов:* – *название улицы, номер дома;* – *название населенного пункта (города, поселка и т.п.);* – *название района;* – *название республики, края, области, автономного округа (области);* – *почтовый индекс* Сегментов нет [*указываются в случае наличия вместе с адресами размещения*]
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	Связь
1.4.	Назначение объекта	Передача информации между автоматизированными системами управления и мониторинга сетей связи и телекоммуникационным оборудованием сетей связи
1.5.	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	Управление и эксплуатация ресурсов (RM&O)
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	Сеть передачи данных

№	Параметр	Сведения
2.	Сведения о субъекте критической информационной инфраструктуры	
2.1.	Наименование субъекта	*Наименование оператора связи*
2.2.	Адрес местонахождения субъекта	*Адрес места государственной регистрации оператора связи:* *– название улицы, номер дома;* *– название населенного пункта (города, поселка и т.п.);* *– название района;* *– название республики, края, области, автономного округа (области);* *– почтовый индекс*
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	*Должность, фамилия, имя, отчество*
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	*Должность, фамилия, имя, отчество*
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	*Наименование структурного подразделения* [*указывается в случае наличия данного подразделения*], *Должность руководителя подразделения* [*указывается в случае наличия данного подразделения*] *или штатного специалиста,* *фамилия, имя, отчество,* *телефон,* *адрес электронной почты*
3.	Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи	
3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Общего пользования [*указываются иные категории сетей электросвязи в случае наличия взаимодействия*]
3.2.	Наименование оператора связи	*Наименование оператора связи* [*это сам оператор связи, т.к. с его сетью электросвязи взаимодействует объект КИИ*]
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнитель-	Передача (прием) информации

№	Параметр	Сведения
	ными устройствами), иная цель)	
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	Тип доступа: Проводной, беспроводной. Технология доступа: xDSL, FE, P2P fiber. Протокол взаимодействия: протоколы стека TCP/IP [*может быть уточнено по решению оператора связи*]
4.	Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры	
4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	[*Ввести сквозную нумерацию эксплуатантов*] *1. Наименование оператора связи* [*если оператор связи сам эксплуатирует объект КИИ*] *2. Название юридического лица* [*если оно эксплуатирует объект КИИ*]. *3. Фамилия, имя, отчество индивидуального предпринимателя* [*если он эксплуатирует объект КИИ*]
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	[*Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*] *1. Адрес:* *– название улицы, номер дома;* *– название населенного пункта (города, поселка и т.п.);* *– название района;* *– название республики, края, области, автономного округа (области);* *– почтовый индекс* *2. Адрес: …*
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	[*Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*] *1. Элементы:* < активное сетевое оборудование уровня core > < активное сетевое оборудование уровня access > < активное сетевое оборудование уровня edge > *< иные компоненты >* [*указываются в случае наличия*] *2. Элементы: …*
5.	Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры	
5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	*Наименования программно-аппаратных средств (активное сетевое оборудование уровня core) и их количество (шт.)*
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операци-	*Наименования общесистемного программного обеспечения (активное сетевое оборудование*

№	Параметр	Сведения
	онных систем, средств виртуализации (при наличии)	*уровня core)*
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	Не применимо
5.4.	Применяемые средства защиты информации (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки; функции безопасности программного обеспечения, если в него встроены средства защиты информации (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции) или сведения об отсутствии средств защиты информации.	*Наименования средств защиты информации* (< *номер и дата выдачи сертификата(ов) соответствия* > или < *номер и дата документа, содержащего результаты оценки соответствия* > или < *оценка соответствия не проводилась* >) [*указывается на каждое средство*] *Идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции* [*указываются в случае наличия*]
6.	Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры	
6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	Внешние и внутренние нарушители, оснащенные в т.ч. средствами, сделанными на заказ, с компетенцией профессионалов, со знанием чувствительной информации и с достаточной мотивацией для реализации угроз безопасности информации согласно «Методическим рекомендациям по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи» (шифр: «КИИ-С-ССОП»)
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	1. Угрозы создания нештатных режимов работы. 2. Угрозы доступа (проникновения) в операционную среду. 2.1. Угрозы непосредственного доступа. 2.1.1. Угрозы, реализуемые в ходе загрузки ОС. 2.1.2. Угрозы, реализуемые после загрузки ОС, независимо от того, какая программа запускается пользователем. 2.1.3. Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. 2.2. Угрозы удаленного доступа (сетевые атаки). 2.2.1. Анализ сетевого трафика. 2.2.2. Сканирование сети. 2.2.3. «Парольная» атака. 2.2.4. Подмена доверенного объекта сети.

№	Параметр	Сведения
		2.2.5.Навязывание ложного маршрута. 2.2.6.Внедрение ложного объекта сети. 2.2.7.Отказ в обслуживании. 2.2.8.Удаленный запуск приложений. 3. Угрозы программно-математического воздействия Реализация угроз < *может привести* > *или* < *не может привести* > к прекращению или нарушению функционирования сети связи
7.	Возможные последствия в случае возникновения компьютерных инцидентов	
7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	1. Отказ в обслуживании. 2. Несанкционированный доступ. 3. Утечка данных (нарушение конфиденциальности). 4. Модификация (подмена) данных. 5. Нарушение функционирования технических средств. 6. Несанкционированное использование вычислительных ресурсов объекта Возникающие инциденты < *могут привести* > *или* < *не могут привести* > к прекращению или нарушению функционирования сети связи
7.2.	Ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" или обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов	Социальный «Прекращение или нарушение функционирования сети связи» (*количество абонентов, зона обслуживания*). Политический «Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)» (*наименование органа(ов) государственной власти, указывается в случае наличия соответствующего действующего государственного контракта*). Экономический «Возникновение ущерба бюджетам Российской Федерации» (*значения потенциально возможных ущербов бюджетам, тыс. рублей и процент*) < *Экологический* > *или* < *Для обороны страны, безопасности государства и правопорядка* > *с соответствующими показателями и значениями* [*если рассмотрены соответствующие виды негативных последствий*]
8.	Категория значимости, которая присвоена объекту критической информационной инфраструктуры	
8.1.	Категория значимости, которая присвоена объекту	< *I категория* > < *II категория* > < *III категория* > < *Отсутствует необходимость присвоения одной из категорий значимости* >

№	Параметр	Сведения
8.2.	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	4. а) Территория, на которой возможно прекращение или нарушение функционирования сети связи: *указать наименование субъекта(ов) РФ (зону обслуживания данным объектом КИИ).* 4. б) Количество людей, для которых могут быть недоступны услуги связи: *указать количество абонентов (тысяч).* 6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия): *указать наименование органа(ов) государственной власти (указывается в случае наличия соответствующего действующего государственного контракта).* 9. а) Снижение доходов федерального бюджета*: указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах.* 9. б) Снижение доходов бюджета субъекта РФ: *указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах* [*указываются последовательно для всех субъектов РФ, входящих в зону обслуживания данным объектом КИИ*] 9. в) Не возникает снижение доходов бюджетов государственных внебюджетных фондов вследствие компьютерных атак на объект КИИ [*Информация о неприменимости остальных показателей приведена в приложении Ж, требуется ее сюда скопировать, в случае их неприменимости; если показатель применим, то требуется указать и показатель, и полученное по нему значение*]
9.	Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры	
9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	Установлена контролируемая зона. Обеспечен контроль физического доступа к объекту КИИ. Разработаны документы (регламенты, инструкции, руководства): – *Название и реквизиты документа;* – *Название и реквизиты документа* *Иные меры* [*указываются в случае наличия*]
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	*Меры:* – *идентификация и аутентификация (ИАФ);* – *управление доступом (УПД);* – *ограничение программной среды (ОПС);* – *защита машинных носителей информации (ЗНИ);* – *аудит безопасности (АУД);* – *антивирусная защита (АВЗ);*

№	Параметр	Сведения
		– предотвращение вторжений (компьютерных атак) (СОВ); *– обеспечение целостности (ОЦЛ);* *– обеспечение доступности (ОДТ);* *– защита технических средств и систем (ЗТС);* *– защита информационной (автоматизированной) системы и ее компонентов (ЗИС).*

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	N докум.	Входящий N сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					