Проект



**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ Российской Федерации**

**П Р И К А З**

\_\_\_\_ \_\_\_\_\_\_\_ 2021 г. Москва № \_\_\_\_\_\_

**Об определении порядка защиты сетей связи и информационных систем операторов связи от несанкционированного доступа к ним и передаваемой по ним информации при функционировании системы обеспечения вызова экстренных оперативных служб по единому номеру «112»**

В соответствии с подпунктом 1 пункта 3 статьи 6 Федерального закона   
от 30 декабря 2020 г. № 488-ФЗ «Об обеспечении вызова экстренных оперативных служб по единому номеру «112» и о внесении изменений в отдельные законодательные акты Российской Федерации» (Собрание законодательства Российской Федерации, 2021, № 1, ст. 27) и, пунктом 5.2.26 Положения   
о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418 (Собрание законодательства Российской Федерации, 2008, № 23, ст. 2708, 2021, № 26, 4967).

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемый Порядок защиты сетей связи и информационных систем операторов связи от несанкционированного доступа к ним и передаваемой по ним информации при функционировании системы обеспечения вызова экстренных оперативных служб по единому номеру «112».
2. Настоящий приказ вступает в силу с 1 сентября 2022 и действует   
   в течении шести лет.

М.И. Шадаев

УТВЕРЖДЕН  
приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации  
от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_

**Порядок защиты сетей связи и информационных систем операторов связи от несанкционированного доступа к ним и передаваемой по ним информации при функционировании системы обеспечения вызова экстренных оперативных служб по единому номеру «112»**

1. Общие положения
2. Настоящий Порядок распространяется на сети связи   
   и информационные системы операторов связи, взаимодействующие в системе обеспечения вызова экстренных оперативных служб по единому номеру «112»   
   (далее соответственно – система-112).
3. Настоящий Порядок является обязательным для всех участников взаимодействия в системе-112.
4. Порядок защиты сетей связи и информационных систем операторов связи от несанкционированного доступа к ним и передаваемой по ним информации при функционировании системы-112
5. Информационная безопасность системы-112, включая защиту информации предоставляемой операторами связи, в пределах объектов автоматизации деятельности системы-112, обеспечивается оператором   
   системы-112 субъекта Российской Федерации в соответствии   
   с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 31.07.2006, № 31, ст. 3448, 2021,   
   № 1, ст. 18), Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 31.07.2006,   
   № 31, ст. 3451, 2021, № 1, ст. 27, ст. 5159).
6. Информационная безопасность сети связи, информационных систем оператора связи и инфраструктуры оператора связи обеспечивается оператором связи в соответствии с Федеральным законом от 7 июля 2003 г. № 126-ФЗ   
   «О связи» (Собрание законодательства Российской Федерации, 2003, № 28,   
   ст. 2895, 2021, № 1, ст. 27), Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом Мининформсвязи России от 9 января 2008 г. №1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним   
   и передаваемой посредством их информации» (Бюллетень нормативных актов федеральных органов исполнительной власти, 2008, № 9), постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687   
   «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (Собрание законодательства Российской Федерации, 2008, № 38, ст. 4320), постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119   
   «Об утверждении требований к защите персональных данных при их обработке   
   в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257), постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии   
   с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» (Собрание законодательства Российской Федерации, 2012, № 14, ст. 1626, 2019, № 16, ст. 1957), приказом ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных   
   с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (Российская газета, 2014, № 211,), приказом ФСТЭК России   
   от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Российская газета, 2013, № 107, Официальный интернет-портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)), 2020), Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства российской Федерации, 31.07.2017, № 31, ст. 4736), приказом ФСТЭК России от 25.12.2017 № 239   
   «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (Официальный интернет-портал правовой информации (www.pravo.gov.ru), 2018, 27 марта), приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г.   
   № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (Российская газета, 2013, № 208) , приказом Минкомсвязи России   
   от 25 июня 2018 г. № 319 «Об утверждении Правил применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VII. Правила применения оборудования коммутации стандарта LTE» (Официальный интернет-портал правовой информации (www.pravo.gov.ru), 2018, 31 июля), приказом Минкомсвязи России от 27 июня 2011 г. № 160 «Об утверждении Правил применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VI. Правила применения узлов связи с территориально распределительной архитектурой стандартов UMTS и/или GSM 900/1800» ("Бюллетень нормативных актов федеральных органов исполнительной власти", № 37, 2011, 12 сентября).
7. При предоставлении оператором связи информации о месте нахождения пользовательского оборудования посредством инициативной передачи информации в сообщениях межстанционной и абонентской телефонной сигнализации, а также при доведении коротких текстовых сообщений (SMS)   
   от пользователей сети связи общего пользования в систему-112, защита сети связи и передаваемой посредством нее информации обеспечивается оператором связи в соответствии с приказом Минкомсвязи России от 1 декабря 2016 г.   
   № 607 «Об утверждении Правил определения места нахождения пользовательского оборудования (оконечного оборудования), с которого были осуществлены вызов или передача сообщения о происшествии по единому номеру вызова экстренных оперативных служб «112», и Порядка предоставления   
   и объема информации, необходимой для обеспечения реагирования по вызову или сообщению о происшествии по единому номеру вызова экстренных оперативных служб «112» (Официальный интернет-портал правовой информации (www.pravo.gov.ru), 2017).
8. Разграничение областей ответственности и физическое сопряжение информационных систем оператора связи, оказывающего услуги связи   
   в соответствии с лицензионными требованиями на оказание услуг связи,   
   и оператора системы-112 субъекта Российской Федерации в части предоставления по запросу информации, необходимой для обеспечения реагирования по вызову или сообщению о происшествии по единому номеру вызова экстренных оперативных служб «112» и доведения коротких текстовых сообщений в систему-112, производится в точке присоединения, системы-112 к сети оператора связи.
9. Каналы передачи данных от центра обработки вызовов системы-112 (далее – ЦОВ-112) (либо конструктивно обособленных технических средств обработки информации о месте нахождения пользовательского (оконечного) оборудования, при наличии) до точки присоединения обеспечивает оператор   
   системы-112, если иное не определено по соглашению сторон.
10. Оператор связи в соответствии с лицензионными требованиями   
    на оказание услуг связи обязан организовать в своей сети связи точку присоединения для систем экстренных оперативных служб. Работоспособность средств связи, составляющих точку присоединения обеспечиваются оператором связи в соответствии с Приказом Мининформсвязи РФ от 27 сентября 2007 г.   
    № 113 "Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования" (Зарегистрировано в Минюсте РФ 22 октября 2007 г. № 10380).
11. В целях защиты передаваемых в рамках информационного взаимодействия системы-112 с информационными системами операторов связи (далее – межсистемное взаимодействие) конфиденциальных и иных охраняемых в соответствии с законодательством Российской Федерации сведений, в том числе персональных данных, должны применяться средства криптографической защиты информации, имеющие подтверждение соответствия требованиям   
    по безопасности информации, установленным федеральным органом исполнительной власти в области обеспечения безопасности (далее – СКЗИ),   
    по классу не ниже КС3.
12. В целях организации защищенного информационного взаимодействия оператор системы-112 предоставляет оператору связи информацию   
    об используемых СКЗИ, необходимую для организации межсистемного взаимодействия.
13. Оператор связи обеспечивает в своей зоне ответственности установку   
    и эксплуатацию однотипного СКЗИ с системой-112 в конфигурации, достаточной   
    для обеспечения межсистемного взаимодействия.
14. Эксплуатация СКЗИ должна осуществляться в соответствии   
    с правилами пользования.
15. Оператор связи определяет правила идентификации и аутентификации при организации доступа технических средств системы-112 к своей информационной системе. Оператор системы-112 определяет, администрирует   
    и передает оператору связи параметры протокола межсистемного информационного взаимодействия.
16. По соглашению оператора связи и оператора системы-112 допускается размещение СКЗИ оператора связи на территории ЦОВ-112 субъекта Российской Федерации.
17. Защита от несанкционированного доступа к абонентским линиям связи при подключении ЦОВ-112 и/или единой диспетчерской службы обеспечивается: при применении радиоэлектронных средств защитным кодированием (шифрованием) информации в радиоканале, для проводных абонентских линий - в соответствии с постановлением Правительства Российской Федерации   
    от 9 июня 1995 г. № 578 «Об утверждении Правил охраны линий и сооружений связи Российской Федерации».
18. Система-112 взаимодействует с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак   
    в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ   
    «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства российской Федерации, 31.07.2017,   
    № 31, ст. 4736), Указом Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак   
    на информационные ресурсы Российской Федерации» (Собрание законодательства Российской Федерации, 25.12.2017, № 52, ст. 8112), Приказом ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» (Официальный интернет-портал правовой информации (www.pravo.gov.ru), 2018), Приказом ФСБ России от 24 июля 2018 г. № 367 «Об утверждении Перечня информации, представляемой   
    в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак   
    на информационные ресурсы Российской Федерации» (Официальный интернет-портал правовой информации (www.pravo.gov.ru), 2018), Приказом ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией   
    о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (Официальный интернет-портал правовой информации (www.pravo.gov.ru), 2018), Приказом ФСБ России от 19 июня 2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных   
    для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» (Официальный интернет-портал правовой информации (www.pravo.gov.ru), 2019) и приказом ФСБ России от 19 июня 2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер   
    по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» (Официальный интернет-портал правовой информации (www.pravo.gov.ru), 2019).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_