Республика Молдова

ПРАВИТЕЛЬСТВО

ПОСТАНОВЛЕНИЕ № HG483/2026
от 26.08.2026

об утверждении методологической базы по оценке рисков для национальных критических инфраструктур, планам безопасности управляющих национальной критической инфраструктурой и деятельности офицера связи по безопасности национальной критической инфраструктуры

Опубликован : 22.09.2026 в MONITORUL OFICIAL № 466-469 статья № 525 Data intrării în vigoare

На основании пункта b) части (2) статьи 7 Закона №223/2025 об идентификации, назначении и защите национальной критической инфраструктуры (Официальный монитор Республики Молдова, 2025 г., № 445–447, ст. 608) Правительство ПОСТАНОВЛЯЕТ:

1. Утвердить методологическую базу по оценке рисков для национальных критических инфраструктур, планам безопасности управляющих национальной критической инфраструктурой и деятельности офицера связи по безопасности национальной критической инфраструктуры, включающую:

1.1. Методологические нормы оценки рисков для национальных критических инфраструктур согласно приложению № 1;

1.2. Методологические нормы разработки, согласования и утверждения Плана безопасности управляющего национальной критической инфраструктурой согласно приложению № 2;

1.3. Типовую структуру Плана безопасности управляющего национальной критической инфраструктурой согласно приложению № 3;

1.4. Методологические нормы признания существующих документов эквивалентными Плану безопасности управляющего национальной критической инфраструктурой согласно приложению № 4;

1.5. Методологические нормы пересмотра и обновления Плана безопасности управляющего национальной критической инфраструктурой согласно приложению № 5;

1.6. Методологические нормы, определяющие порядок назначения, функциональный статус и обязанности офицера связи по безопасности национальной

критической инфраструктуры, согласно приложению № 6.

2. Министерству внутренних дел посредством Национального центра по координации защиты критических инфраструктур обеспечить методологическую координацию, мониторинг и оказание специализированной помощи в применении настоящего постановления.

3. Для целей настоящего постановления ответственными органами публичной власти являются органы, назначенные Постановлением Правительства № 185/2026 о назначении органов публичной власти, ответственных за секторы и подсекторы национальной критической инфраструктуры.

4. Ответственным органам публичной власти применять положения настоящего постановления в секторах и подсекторах, за которые они несут ответственность, согласовывать планы безопасности управляющих национальной критической инфраструктурой и осуществлять мониторинг соблюдения указанными управляющими требований законодательства и методологических требований.

5. Управляющим национальной критической инфраструктурой обеспечить разработку, утверждение, направление на согласование, реализацию, тестирование, пересмотр и обновление планов безопасности в соответствии с Законом № 223/2025 об идентификации, назначении и защите национальной критической инфраструктуры и методологической базой, утвержденной настоящим постановлением.

6. Имеющиеся у управляющих национальной критической инфраструктурой документы, регламентирующие меры в области безопасности, обеспечения непрерывности деятельности, физической защиты, кибербезопасности, реагирования на инциденты, гражданской защиты или иные соответствующие меры, могут быть полностью или частично признаны эквивалентными Плану безопасности управляющего национальной критической инфраструктурой на условиях, установленных настоящим постановлением.

7. Ответственным органам публичной власти разработать отраслевые инструкции, руководства, образцы документов или внутренние процедуры, необходимые для применения настоящего постановления в секторах и подсекторах, за которые они несут ответственность, с соблюдением требований методологической базы, утвержденной настоящим постановлением, и проинформировать об этом Национальный центр по координации защиты критических инфраструктур.

8. Если для одного и того же сектора или подсектора национальной критической инфраструктуры назначены два или более ответственных органа публичной власти, обязанности, предусмотренные в пунктах 4 и 7, исполняются каждым из них в пределах установленных законом полномочий и в сфере, за которую он несет ответственность. По общим и взаимосвязанным вопросам, а также вопросам, касающимся всего сектора или подсектора, ответственным органам публичной власти обеспечить координацию действий, обмен информацией и, при необходимости, совместную разработку отраслевых инструкций, руководств, образцов документов или процедур, необходимых для применения настоящего постановления, и

проинформировать об этом Национальный центр по координации защиты критических инфраструктур.

9. Министерствам, административным органам, подведомственным министерствам, другим центральным административным органам и ответственным публичным учреждениям в течение 12 месяцев с даты вступления в силу настоящего постановления привести ведомственные нормативные акты, внутренние процедуры и применяемые документы в соответствие с ним; при этом управляющие национальной критической инфраструктурой обязаны разработать и направить на согласование план безопасности в срок, предусмотренный методологической базой, утвержденной настоящим постановлением.

10. Контроль за выполнением настоящего постановления возложить на Министерство внутренних дел.

11. Настоящее постановление вступает в силу с даты опубликования в Официальном мониторе Республики Молдова.

ПРЕМЬЕР-МИНИСТР Василе ТОФАН

Контрассигнует:

Министр внутренних дел Даниелла Мисаил-Никитин

№ 483. Кишинэу, 26 августа 2026 г.

Приложение № 1

к Постановлению Правительства

№ 483/2026

МЕТОДОЛОГИЧЕСКИЕ НОРМЫ

оценки рисков для национальных критических инфраструктур

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Методологические нормы регулируют порядок организации, проведения, документального оформления и обновления оценки рисков для национальных критических инфраструктур.

2. Оценка рисков для национальных критических инфраструктур представляет собой структурированный процесс, в ходе которого осуществляются выявление, анализ, оценка, определение приоритетности и мониторинг рисков, а также представление отчетности о рисках, которые могут повлиять на национальную критическую инфраструктуру, критические функции, критические активы, основные процессы либо непрерывность предоставления посредством нее основной услуги.

3. Целью оценки рисков является обоснование мер безопасности, защиты, предупреждения, обеспечения непрерывности, реагирования и восстановления, подлежащих включению в План безопасности управляющего национальной критической инфраструктурой (в дальнейшем – *План безопасности*).

4. Настоящие Методологические нормы применяются к управляющим национальными критическими инфраструктурами (в дальнейшем – *управляющие*), назначенными в соответствии с законом, независимо от вида собственности, организационно-правовой формы или сектора деятельности.

5. Настоящие Методологические нормы применяются в пределах установленных законом полномочий к ответственным органам публичной власти, компетентным органам и иным субъектам, участвующим в процессе оценки рисков, согласования, мониторинга или использования результатов оценки рисков.

6. Оценка рисков проводится в отношении каждой назначенной национальной критической инфраструктуры с учетом специфики соответствующих сектора и подсектора, предоставляемой основной услуги, критических компонентов, местонахождения, среды функционирования, зависимостей, взаимозависимостей и степени подверженности угрозам и опасностям.

7. Оценка рисков является обязательной основой для разработки, обновления и пересмотра Плана безопасности.

8. Применение настоящих Методологических норм не затрагивает специальные обязательства, предусмотренные законодательством, применимым к соответствующему сектору или подсектору, законодательством в области кибербезопасности, защиты информации, кризисных ситуаций, гражданской защиты, противопожарной защиты, безопасности и гигиены труда, предупреждения и контроля экологических рисков, а также иными применимыми специальными нормативными актами.

9. Применение настоящих Методологических норм осуществляется с соблюдением следующих принципов:

9.1. законности;

9.2. комплексного подхода;

9.3. предупреждения;

9.4. подхода, основанного на оценке рисков;

9.5. пропорциональности;

9.6. непрерывности предоставления основных услуг;

9.7. институционального сотрудничества;

9.8. прослеживаемости;

9.9. конфиденциальности и защиты информации;

9.10. периодического пересмотра и постоянного совершенствования.

10. В настоящих Методологических нормах термины и выражения используются в значении, установленном в Законе № 223/2025 об идентификации, назначении и защите национальной критической инфраструктуры, а также в нормативных актах в области управления рисками, национальной безопасности, кибербезопасности, кризисных ситуаций и защиты информации.

II. ОРГАНИЗАЦИЯ ПРОЦЕССА ОЦЕНКИ РИСКОВ

11. Оценка рисков проводится управляющим национальной критической инфраструктурой в сотрудничестве с ответственным органом публичной власти соответствующего сектора или подсектора. Национальный центр по координации защиты критических инфраструктур (в дальнейшем – *НЦКЗКИ*) при необходимости оказывает методологическую поддержку ответственным органам публичной власти и управляющим национальными критическими инфраструктурами при применении настоящих Методологических норм.

12. Ответственный орган публичной власти может устанавливать дополнительные требования к оценке рисков при условии соблюдения методологической базы, утвержденной настоящим постановлением, и уведомления НЦКЗКИ.

13. Процесс оценки рисков начинается:

13.1. после назначения инфраструктуры в качестве национальной критической инфраструктуры;

13.2. при разработке Плана безопасности;

13.3. при обновлении оценки рисков;

13.4. после крупного инцидента или значительного нарушения;

13.5. в случае изменения угроз, уязвимых мест, зависимостей или взаимозависимостей, имеющих значение для оценки рисков;

13.6. в случае изменения технической или функциональной конфигурации, правового статуса либо организационной структуры национальной критической инфраструктуры;

13.7. по запросу ответственного органа публичной власти или НЦКЗКИ в соответствии с законом.

14. Управляющий назначает лиц или подразделения, ответственные за проведение оценки рисков.

15. К процессу оценки рисков при необходимости могут привлекаться

представители подразделений, отвечающих за физическую безопасность, кибербезопасность, непрерывность деятельности, гражданскую защиту, чрезвычайные ситуации, техническое обслуживание, техническую эксплуатацию, логистику, управление человеческими ресурсами, правовое обеспечение, коммуникацию и оперативное управление.

16. Для проведения оценки рисков, требующей специальных знаний, управляющий или ответственный орган публичной власти может запросить содействие экспертов либо компетентных структур с соблюдением режима защиты чувствительной информации или информации, отнесенной к государственной тайне.

III. ОБЪЕКТ ОЦЕНКИ РИСКОВ

17. Объектом оценки рисков являются назначенная национальная критическая инфраструктура во всей совокупности ее функций, а также основная услуга, предоставление которой обеспечивается данной инфраструктурой.

18. Оценка рисков в соответствующих случаях охватывает:

18.1. инфраструктуру и относящиеся к ней установки, оборудование, сети, системы и подсистемы;

18.2. материальные и нематериальные активы, имеющие ключевое значение;

18.3. критические функции и операционные процессы, необходимые для функционирования инфраструктуры;

18.4. ключевой персонал и необходимые профессиональные компетенции;

18.5. информационные системы, средства связи и иные цифровые или технологические компоненты;

18.6. зависимость от поставщиков товаров и услуг, цепочек поставок и иных внешних факторов;

18.7. взаимозависимости с другими критическими инфраструктурами, основными услугами либо системами публичного или частного сектора;

18.8. места размещения, узлы, соединения и иные элементы, без которых невозможно обеспечить непрерывность предоставления основной услуги или возобновить ее предоставление в приемлемый срок.

19. Объект оценки рисков четко определяется исходя из:

19.1. физических и функциональных границ национальной критической инфраструктуры;

19.2. предоставляемой основной услуги или предоставляемых основных услуг;

19.3. минимально допустимых параметров функционирования;

19.4. условий обеспечения непрерывности, функционирования в ограниченном режиме и восстановления;

19.5. периода анализа и исходных допущений.

IV. ЭТАПЫ ОЦЕНКИ РИСКОВ

20. Оценка рисков, проводимая управляющим, включает по меньшей мере следующие этапы:

20.1. определение границ объекта оценки;

20.2. выявление основной услуги, критических функций, критических активов и основных процессов;

20.3. выявление угроз, опасностей, опасных факторов, источников риска и факторов, способных привести к его возникновению;

20.4. выявление уязвимых мест;

20.5. выявление зависимостей и взаимозависимостей;

20.6. разработка сценариев риска;

20.7. оценка воздействия;

20.8. оценка вероятности;

20.9. определение балла и уровня риска;

20.10. определение приоритетности рисков;

20.11. выявление действующих мер и оценка их эффективности, а также определение дополнительных мер по управлению рисками и приоритетности их реализации;

20.12. документирование результатов.

21. Оценка рисков на этапах, предусмотренных пунктом 20, проводится с соблюдением принципа пропорциональности, с учетом характера национальной критической инфраструктуры, степени ее сложности, сектора, к которому она относится, и уровня оцениваемых рисков.

22. На этапе выявления критических функций, критических активов и основных процессов управляющий определяет элементы, без которых национальная критическая инфраструктура не может предоставлять основную услугу либо возобновить ее предоставление.

23. Для каждой критической функции выявляются по меньшей мере:

23.1. связанные с ней критические активы;

23.2. основные процессы и операционные потоки;

23.3. ключевой персонал и необходимые профессиональные компетенции;

23.4. необходимые логистические, энергетические, информационные и технологические ресурсы;

23.5. внутренние и внешние зависимости.

24. Управляющий выявляет все значимые категории угроз, опасностей, опасных факторов, инцидентов и источников риска, которые могут повлиять на национальную критическую инфраструктуру или предоставление основной услуги.

25. Угрозы, опасности и источники риска выявляются на основании:

25.1. данных о ранее произошедших инцидентах и нарушениях;

25.2. внутреннего и секторального анализа;

25.3. информации, предоставленной компетентными органами и ответственными органами публичной власти;

25.4. соответствующих технических, статистических и научных отчетов;

25.5. выводов по результатам учений, аудитов и проверок, а также анализа ранее произошедших событий;

25.6. анализа изменений среды рисков и появления новых уязвимых мест;

25.7. национальной оценки рисков, стратегических оценок и иных соответствующих документов, разработанных в рамках Национальной системы управления кризисами.

26. Управляющий выявляет уязвимые места физического, технического, технологического, организационного, кадрового, информационного и кибернетического характера, а также любые иные недостатки, которые могут способствовать реализации риска или усугублению его последствий.

27. Отдельно выявляются:

27.1. структурные и обусловленные местом размещения уязвимые места;

27.2. операционные и процедурные уязвимые места;

27.3. уязвимые места, обусловленные персоналом, недостатком компетенций или ненадлежащим доступом;

27.4. уязвимые места, относящиеся к информационным и технологическим системам;

27.5. уязвимые места, обусловленные внешними зависимостями, поставщиками

или цепочкой поставок;

27.6. уязвимые места, возникающие вследствие взаимозависимости с другими критическими инфраструктурами или основными услугами.

28. В отношении выявленных рисков управляющий разрабатывает реалистичные, значимые и документально обоснованные сценарии риска, в которых описываются возможные способы реализации риска и его потенциальные последствия для национальной критической инфраструктуры и основной услуги.

29. Сценарии риска в соответствующих случаях включают:

29.1. источник риска или фактор, способствующий его возникновению;

29.2. уязвимые места, которые могут быть использованы для реализации риска либо затронуты им;

29.3. вероятную последовательность событий;

29.4. прямые и косвенные последствия;

29.5. предполагаемую продолжительность нарушения;

29.6. воздействие на критические функции, критические активы и основную услугу;

29.7. последствия распространения и взаимозависимости.

V. КАТЕГОРИИ АНАЛИЗИРУЕМЫХ РИСКОВ

30. Оценка рисков для национальных критических инфраструктур проводится с учетом всех значимых категорий рисков, которые могут прямо или косвенно повлиять на национальную критическую инфраструктуру, критические функции, критические активы, основные процессы либо непрерывность предоставления основной услуги.

31. Оценка в соответствующих случаях охватывает следующие категории рисков:

31.1. природные риски, включая землетрясения, наводнения, бури, экстремальные температуры, засуху, природные пожары, оползни, опасные метеорологические явления, эпидемии, пандемии и иные природные и биологические явления, способные вызвать нарушения;

31.2. технологические и промышленные риски, включая аварии, взрывы, пожары, серьезные неисправности, технические сбои, аварии в ходе технологических процессов, ошибки проектирования или технического обслуживания;

31.3. преднамеренные антропогенные риски, включая саботаж, терроризм, грубый вандализм, несанкционированное проникновение, кражу, умышленное уничтожение или нарушение безопасности;

31.4. гибридные риски, включая скоординированные или комбинированные действия, направленные на нарушение функционирования национальной критической инфраструктуры с использованием физических, информационных, экономических, социальных, кибернетических или психологических средств;

31.5. киберриски, включая кибератаки, нарушение безопасности систем управления, нарушение работы сетей, а также целостности, конфиденциальности или доступности данных и услуг;

31.6. организационные и кадровые риски, включая ошибки персонала, нехватку ключевых работников, недостаток необходимых компетенций, несанкционированный доступ, внутренние конфликты, коррупцию, несоблюдение установленных процедур или реорганизацию;

31.7. риски, связанные с цепочкой поставок и внешними зависимостями, включая перебои в поставках, недоступность сырья, энергоснабжения, средств связи, технической поддержки или иных критически важных ресурсов;

31.8. репутационные или информационные риски в той мере, в которой они могут повлиять на непрерывность предоставления основной услуги, доверие общественности, оперативное взаимодействие или способность к реагированию;

31.9. иные риски, характерные для соответствующего сектора и оцениваемой национальной критической инфраструктуры.

32. В случае гибридных рисков и рисков с системным воздействием оценка включает анализ потенциальных последствий для непрерывности жизненно важных функций государства, функционирования других секторов и национальных критических инфраструктур, а также национальной устойчивости.

33. В процессе оценки управляющий разграничивает:

33.1. угрозы, представляющие собой риски, связанные с преднамеренными, враждебными или умышленными действиями;

33.2. опасности либо опасные явления, представляющие собой события, процессы или явления, не обусловленные враждебными намерениями какого-либо субъекта.

34. Разграничение, предусмотренное пунктом 33, применяется при выборе методов оценки вероятности и надлежащем описании сценариев риска.

VI. ОЦЕНКА ВОЗДЕЙСТВИЯ

35. При оценке воздействия каждого риска учитываются возможные последствия:

35.1. для жизни, здоровья и безопасности людей;

35.2. для непрерывности предоставления основной услуги и функционирования

национальной критической инфраструктуры;

35.3. для экономики и финансовой деятельности;

35.4. для окружающей среды;

35.5. для общественного порядка и общественной безопасности;

35.6. для национальной безопасности и способности государства осуществлять управление;

35.7. для репутации организации и выполнения соответствующих обязательств;

35.8. межсекторального или каскадного характера.

36. Воздействие оценивается по единой пятиуровневой шкале от 1 до 5 следующим образом:

36.1. уровень 1 – очень низкое воздействие: последствия, с которыми управляющий может справиться с использованием имеющихся ресурсов, без существенного ущерба охраняемым ценностям, значительных перерывов в предоставлении основной услуги и каскадных эффектов;

36.2. уровень 2 – низкое воздействие: ограниченные контролируемые нарушения, оказывающие незначительное и временное воздействие на отдельный компонент инфраструктуры, небольшую группу населения или ограниченный сегмент основной услуги и не влекущие серьезных последствий для функционирования инфраструктуры в целом;

36.3. уровень 3 – умеренное воздействие: серьезные последствия для отдельного региона, оператора, жизненно важного сектора или непрерывности предоставления услуги в обычном режиме, приводящие к нарушению текущего функционирования и требующие принятия дополнительных оперативных и управленческих мер;

36.4. уровень 4 – высокое воздействие: масштабные нарушения, серьезно затрагивающие критические функции, создающие угрозу гибели значительного числа людей, причинения значительного экономического ущерба, одновременного ущерба нескольким охраняемым ценностям или значительного распространения последствий на другие системы либо секторы;

36.5. уровень 5 – критическое воздействие: катастрофические последствия, массовая гибель людей, масштабное прекращение предоставления основных услуг, нарушение жизненно важных функций либо невозможность поддерживать предоставление основной услуги на минимально допустимом уровне.

37. Если сценарий риска одновременно затрагивает несколько областей воздействия, итоговая оценка воздействия определяется:

37.1. как максимальное значение выявленного воздействия, если одно из последствий является преобладающим; или

37.2. как обоснованное совокупное значение, если воздействие в значительной степени распространяется на несколько областей.

38. Выбранный метод определения итоговой оценки воздействия прямо указывается в карточке оценки риска.

VII. ОЦЕНКА ВЕРОЯТНОСТИ

39. Вероятность каждого риска оценивается с учетом характера риска, частоты его реализации либо реалистичности соответствующего сценария, а также имеющихся данных.

40. Вероятность оценивается по единой пятиуровневой шкале от 1 до 5 следующим образом:

40.1. уровень 1 – очень низкая вероятность: сценарий маловероятен; соответствующие прецеденты отсутствуют либо носят исключительный характер; необходимые для его реализации условия возникают редко;

40.2. уровень 2 – низкая вероятность: сценарий возможен, но маловероятен; имеются лишь отдельные признаки или немногочисленные прецеденты; необходимые условия складываются редко;

40.3. уровень 3 – умеренная вероятность: сценарий реалистичен и может осуществиться при определенных условиях; имеются соответствующие уязвимые места или прецеденты; необходимые условия могут складываться периодически;

40.4. уровень 4 – высокая вероятность: сценарий весьма вероятен; имеются существенные признаки, тенденции или уязвимые места; необходимые для его осуществления условия возникают часто или могут легко сложиться;

40.5. уровень 5 – очень высокая вероятность: сценарий может реализоваться в ближайшее время, носит повторяющийся характер либо практически неизбежен при отсутствии дополнительных мер; имеются явные признаки, многочисленные прецеденты или сохраняющиеся критические уязвимые места.

41. Для рисков, относящихся к опасностям или опасным явлениям, вероятность определяется главным образом на основании статистических данных, наблюдаемой частоты, прогнозных моделей, подтвержденных тенденций и сведений о произошедших инцидентах.

42. Для рисков, относящихся к угрозам, вероятность оценивается на основании имеющихся сведений о намерениях, возможностях, степени подверженности, уязвимости, оперативной обстановке и обстановке в сфере безопасности.

VIII. ОПРЕДЕЛЕНИЕ БАЛЛА И УРОВНЯ РИСКА

43. Балл риска рассчитывается путем умножения оценки воздействия на оценку вероятности по следующей формуле:

Балл риска = Воздействие x Вероятность

44. Балл риска может принимать значения от 1 до 25.

45. В целях классификации рисков и определения их приоритетности устанавливаются следующие уровни риска:

45.1. 1–4 – низкий риск;

45.2. 5–10 – умеренный риск;

45.3. 11–15 – высокий риск;

45.4.16–25 – критический риск.

46. Матрица рисков представляет собой таблицу размером 5x5 и используется для распределения, сопоставления и ранжирования рисков.

Воздействие\Вероятность	**1**	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

47. Матрица рисков используется для:

47.1. классификации рисков;

47.2. сопоставления рисков;

47.3. определения приоритетности мер реагирования;

47.4. обоснования мер, предусмотренных Планом безопасности;

47.5. обоснования распределения ресурсов.

IX. ОПРЕДЕЛЕНИЕ ПРИОРИТЕТНОСТИ РИСКОВ

И МЕРЫ ПО УПРАВЛЕНИЮ ИМИ

48. После определения уровня рисков управляющий определяет их приоритетность с учетом степени серьезности, последствий для основной услуги, связанных с ними уязвимых мест, а также имеющихся возможностей по предупреждению, защите, реагированию, обеспечению непрерывности и восстановлению.

49. Меры по управлению высокими и критическими рисками принимаются в

первоочередном порядке.

50. Для каждого приоритетного риска определяются:

50.1. действующие меры безопасности;

50.2. необходимые дополнительные меры;

50.3. очередность их реализации;

50.4. ответственные лица;

50.5. необходимые ресурсы;

50.6. срок реализации;

50.7. показатели выполнения;

50.8. порядок проверки.

51. Управление рисками может предусматривать:

51.1. предотвращение риска;

51.2. снижение вероятности;

51.3. снижение воздействия;

51.4. передачу или разделение риска в соответствующих случаях;

51.5. принятие остаточного риска при наличии обоснования;

51.6. подготовку к реагированию и восстановлению.

52. Меры по управлению рисками могут включать:

52.1. организационные меры;

52.2. технические меры;

52.3. процедурные меры;

52.4. меры физической безопасности;

52.5. меры кибербезопасности;

52.6. меры по обеспечению непрерывности;

52.7. меры оперативного вмешательства и реагирования;

52.8. меры по подготовке персонала и проведению учений;

52.9. меры по обеспечению связи и оповещения;

52.10. меры по резервированию и восстановлению.

53. Управляющий документально оформляет и обосновывает остаточный риск, а также осуществляет его мониторинг.

54. Меры по управлению рисками включаются в План безопасности или в связанные с ним документы.

X. ДОКУМЕНТАЛЬНОЕ ОФОРМЛЕНИЕ ОЦЕНКИ РИСКОВ

55. Результаты оценки рисков отражаются в карточках оценки рисков, составляемых для каждого значимого риска или каждой однородной группы рисков.

56. Карточка оценки риска содержит по меньшей мере:

56.1. наименование риска;

56.2. описание сценария риска;

56.3. затрагиваемые активы, функции и процессы;

56.4. значимые уязвимые места и зависимости;

56.5. оцененные воздействие и вероятность;

56.6. балл и уровень риска;

56.7. действующие меры;

56.8. предлагаемые дополнительные меры;

56.9. источники данных и степень их надежности;

56.10. дату проведения оценки и сведения о лицах, ответственных за ее проведение.

57. Управляющий обеспечивает хранение данных, ссылок на источники, расчетов, сценариев и иных подтверждающих документов, на которых основывалась оценка рисков.

58. Управляющий ведет реестр рисков, содержащий выявленные риски, их баллы и уровни, действующие и дополнительные меры, а также сведения о ходе реализации этих мер.

59. Результаты оценки рисков включаются в отчет об оценке рисков для национальной критической инфраструктуры.

60. Отчет об оценке рисков утверждается руководителем управляющего национальной критической инфраструктурой или уполномоченным им лицом.

61. Отчет об оценке рисков представляется ответственному органу публичной

власти вместе с Планом безопасности или соответствующими документами, запрошенными в процессе согласования.

XI. ОБНОВЛЕНИЕ ОЦЕНКИ РИСКОВ

62. Оценка рисков обновляется не реже одного раза в год в срок, позволяющий использовать ее результаты при подготовке отчетов, предусмотренных частями (2) и (3) статьи 6 Закона №223/2025 об идентификации, назначении и защите национальной критической инфраструктуры, а также при возникновении существенных изменений, касающихся национальной критической инфраструктуры, основной услуги, среды рисков, зависимостей, взаимозависимостей или значимых уязвимых мест.

63. Оценка рисков обновляется по меньшей мере в следующих случаях:

63.1. после крупного инцидента или значительного нарушения;

63.2. после структурных, функциональных, технологических или организационных изменений;

63.3. после значимых изменений цепочки поставок либо внешних зависимостей;

63.4. после проведения аудитов, проверок, учений или испытаний, в ходе которых выявлены несоответствия или новые уязвимые места;

63.5. при возникновении новых угроз или изменении уровня существующих угроз;

63.6. при изменении значимых взаимозависимостей;

63.7. при изменении уровня тревоги или объявлении кризисной ситуации, если это влияет или может повлиять на национальную критическую инфраструктуру либо непрерывность предоставления основной услуги;

63.8. по запросу ответственного органа публичной власти или Национального центра по координации защиты критических инфраструктур в соответствии с законом.

64. Любое существенное изменение, внесенное в оценку рисков, оформляется запиской об обновлении.

65. В записке об обновлении указываются по меньшей мере:

65.1. причина обновления;

65.2. выявленные новые риски;

65.3. изменившиеся риски;

65.4. новые или изменившиеся уязвимые места;

65.5. изменения оценки воздействия или вероятности;

65.6. необходимые дополнительные меры;

65.7. влияние обновления на План безопасности.

66. Если в результате обновления оценки рисков существенно изменяются профиль риска или меры безопасности, управляющий инициирует пересмотр Плана безопасности в соответствии с методологическими нормами его пересмотра и обновления.

XII. ЗАЩИТА ИНФОРМАЦИИ

67. Обращение с информацией, используемой или полученной в процессе оценки рисков, осуществляется с соблюдением правового режима, применимого к информации, отнесенной к государственной тайне, персональным данным, чувствительной информации, касающейся национальных критических инфраструктур, и иным категориям охраняемой законом информации.

68. Доступ к информации об оценке рисков предоставляется в соответствии с принципом необходимости знать и только лицам, непосредственно участвующим в оценке, согласовании, мониторинге, контроле или реализации мер безопасности.

69. Управляющий и ответственный орган публичной власти обеспечивают учет, хранение, передачу, архивирование и, при необходимости, уничтожение документов, связанных с оценкой рисков, в соответствии с законом.

70. Данные об уязвимостях, сценариях рисков, критических взаимозависимостях, мерах безопасности, возможностях реагирования и уязвимых элементах национальной критической инфраструктуры рассматриваются как чувствительная информация и защищаются с учетом уровня риска, возникающего вследствие их разглашения.

71. В отношении критических инфраструктур в сфере обороны, общественного порядка и государственной безопасности сроки и процедуры передачи, проверки и согласования документов устанавливаются с учетом режима защиты информации, отнесенной к государственной тайне, при этом используются исключительно защищенные каналы связи и привлекается персонал, имеющий соответствующий допуск в соответствии с законодательством.

XIII. ОБЩИЕ ПРАВИЛА ПРИМЕНЕНИЯ И МЕТОДОЛОГИЧЕСКОГО СОГЛАСОВАНИЯ

72. Оценка рисков в отношении национальных критических инфраструктур не заменяет оценки рисков, предусмотренные специальным законодательством, а согласуется с ними в целях обеспечения комплексного подхода к безопасности, защите, непрерывности и устойчивости национальных критических инфраструктур.

73. Ответственные органы публичной власти и управляющие сотрудничают в целях обеспечения единого, соразмерного и согласованного подхода в процессе оценки

рисков.

74. НЦКЗКИ разрабатывает и предоставляет ответственным органам публичной власти и управляющим национальными критическими инфраструктурами типовые формы и стандартизированные методологические инструменты для применения настоящих Методологических норм, включая модели оценки рисков, реестры рисков, оценочные матрицы, карточки рисков, типовые формы отчетности, модели пересмотра и иные инструменты, необходимые для единообразного осуществления процесса оценки рисков.

75. Результаты оценки рисков служат основой для плана безопасности управляющего национальной критической инфраструктурой, мер по обработке рисков и процесса его пересмотра.

Приложение № 2

к Постановлению Правительства

№ 483/2026

МЕТОДОЛОГИЧЕСКИЕ НОРМЫ

разработки, согласования и утверждения Плана безопасности управляющего национальной критической инфраструктурой

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Методологические нормы регулируют порядок разработки, направления на согласование, рассмотрения и утверждения Плана безопасности управляющего национальной критической инфраструктурой (в дальнейшем – *План безопасности*).

2. План безопасности представляет собой документ стратегического планирования, имеющий оперативный характер благодаря связанным с ним процедурам, который разрабатывается для каждой назначенной национальной критической инфраструктуры и определяет цели, меры, обязанности, ресурсы и процедуры, необходимые для ее защиты, безопасности, непрерывности функционирования и устойчивости.

3. План безопасности предназначен для воплощения результатов оценки рисков в организационных, технических, процедурных и оперативных мерах, направленных на предупреждение инцидентов, снижение их последствий, управление ими и восстановление после них, если такие инциденты могут затронуть национальную критическую инфраструктуру или предоставляемую посредством нее основную услугу.

4. План безопасности разрабатывается управляющим национальной критической инфраструктурой (в дальнейшем – *управляющий*) для каждой назначенной национальной критической инфраструктуры независимо от его

организационно-правовой формы, формы собственности или сектора деятельности.

5. Если один и тот же управляющий осуществляет управление или эксплуатацию нескольких национальных критических инфраструктур, он вправе:

5.1. разрабатывать отдельные планы безопасности для каждой национальной критической инфраструктуры; или

5.2. разрабатывать единый план при условии четкого, раздельного и поддающегося проверке выделения элементов, относящихся к каждой национальной критической инфраструктуре.

6. Единый план, предусмотренный в подпункте 5.2 пункта 5, должен обеспечивать возможность отдельной идентификации для каждой национальной критической инфраструктуры рисков, критических функций, критических активов, мер безопасности, обязанностей, ресурсов, сроков и применимых процедур.

7. План безопасности разрабатывается на основании:

7.1. оценки рисков, проведенной в соответствии с Методологическими нормами оценки рисков для национальных критических инфраструктур, предусмотренными в приложении № 1;

7.2. нормативной базы, применимой к соответствующему сектору или подсектору;

7.3. типовой структуры, предусмотренной в приложении № 3;

7.4. отраслевых инструкций, изданных ответственным органом публичной власти, в соответствующих случаях;

7.5. установленных законодательством обязательств в области безопасности, обеспечения непрерывности, гражданской защиты, кибербезопасности, антитеррористической защиты, защиты информации и других соответствующих областях;

7.6. выводов, сделанных по итогам инцидентов, учений, тестирований, аудитов или проверок.

8. План безопасности не заменяет планы, процедуры или документы, предусмотренные специальным законодательством, а согласуется с ними и в соответствующих случаях интегрирует их в единый механизм обеспечения защиты, непрерывности и устойчивости национальной критической инфраструктуры.

9. Разработка, согласование и утверждение Плана безопасности осуществляются с соблюдением принципов законности, пропорциональности, подхода, основанного на оценке рисков, ответственности управляющего, институционального сотрудничества, непрерывности основных услуг, прослеживаемости, конфиденциальности и защиты чувствительной информации или информации, отнесенной к государственной тайне.

II. ОТВЕТСТВЕННОСТЬ В ПРОЦЕССЕ РАЗРАБОТКИ ПЛАНА БЕЗОПАСНОСТИ

10. Общая ответственность за разработку, направление на согласование, окончательное утверждение, реализацию, тестирование, пересмотр и обновление Плана безопасности возлагается на управляющего.

11. Руководитель управляющего национальной критической инфраструктурой обеспечивает:

11.1. инициирование процесса разработки Плана безопасности;

11.2. назначение ответственных лиц или структур;

11.3. выделение ресурсов, необходимых для разработки, проведения консультаций, тестирования и обновления;

11.4. предварительное утверждение проекта Плана безопасности в целях его направления на согласование;

11.5. направление Плана безопасности на согласование ответственному органу публичной власти;

11.6. окончательное утверждение Плана безопасности после получения согласования ответственного органа публичной власти;

11.7. реализацию мер, предусмотренных Планом безопасности;

11.8. мониторинг реализации, тестирования, пересмотра и обновления Плана безопасности.

12. Офицер связи по безопасности национальной критической инфраструктуры координирует на оперативном и методологическом уровнях процесс разработки Плана безопасности, при этом ответственность руководства управляющего за данный процесс сохраняется.

13. В разработке Плана безопасности в соответствующих случаях участвуют соответствующие внутренние структуры управляющего, в том числе ответственные за:

13.1. управление и эксплуатацию;

13.2. физическую безопасность;

13.3. информационную и кибербезопасность;

13.4. непрерывность деятельности;

13.5. управление рисками;

13.6. гражданскую защиту и чрезвычайные ситуации;

13.7. человеческие ресурсы;

13.8. правовое обеспечение;

13.9. закупки, логистику, техническое обеспечение и техническое обслуживание;

13.10. публичную коммуникацию;

13.11. защиту информации;

13.12. другие соответствующие области с учетом специфики национальной критической инфраструктуры.

14. Ответственный орган публичной власти обеспечивает отраслевую координацию процесса разработки планов безопасности, предоставляет методологические разъяснения управляющим в сфере своей ответственности и рассматривает планы, направленные на согласование.

15. Национальный центр по координации защиты критических инфраструктур (в дальнейшем – *НЦКЗКИ*) оказывает методологическую поддержку ответственным органам публичной власти и, в соответствующих случаях, управляющим национальными критическими инфраструктурами в целях единообразного применения требований к Планам безопасности.

III. ОБЩИЕ ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ПЛАНА БЕЗОПАСНОСТИ

16. План безопасности разрабатывается в соответствии с типовой структурой, предусмотренной в приложении № 3.

17. План безопасности должен:

17.1. учитывать специфику национальной критической инфраструктуры, для которой он разрабатывается;

17.2. основываться на оценке рисков;

17.3. быть применимым с оперативной точки зрения;

17.4. быть согласованным с соответствующими внутренними документами управляющего;

17.5. быть изложенным в ясной и последовательной форме, позволяющей его обновление;

17.6. быть соразмерным уровню выявленных рисков.

18. План безопасности включает по меньшей мере:

18.1. общие сведения об управляющем и национальной критической

инфраструктуре;

18.2. описание предоставляемой основной услуги;

18.3. описание критических функций, критических активов и основных процессов;

18.4. сводные результаты оценки рисков;

18.5. существующие меры безопасности и обеспечения непрерывности;

18.6. дополнительные меры по обработке рисков;

18.7. процедуры предупреждения, защиты, обнаружения и оповещения;

18.8. процедуры реагирования на инциденты;

18.9. процедуры обеспечения непрерывности и восстановления;

18.10. внутренние и внешние сферы ответственности;

18.11. механизмы коммуникации, уведомления и отчетности;

18.12. ресурсы, необходимые для реализации мер;

18.13. механизмы координации и сотрудничества с компетентными органами в области управления кризисными ситуациями в случае инцидентов, превышающих возможности управляющего по реагированию либо вызывающих системные или межсекторальные последствия;

18.14. график реализации;

18.15. порядок обучения, тестирования и проведения учений;

18.16. порядок мониторинга, пересмотра и обновления;

18.17. технические приложения и вспомогательные документы.

19. Для каждой соответствующей меры, предусмотренной Планом безопасности, указываются:

19.1. описание меры;

19.2. ее цель;

19.3. риск, уязвимость, критическая функция или критический актив, в отношении которых применяется мера;

19.4. лицо, ответственное за реализацию;

19.5. срок реализации или применения;

19.6. необходимые ресурсы, в соответствующих случаях;

19.7. показатель выполнения;

19.8. способ проверки.

20. В отношении рисков, отнесенных к высоким или критическим, План безопасности в обязательном порядке предусматривает конкретные меры по снижению вероятности их реализации, уменьшению воздействия, обеспечению непрерывности и восстановлению.

21. В отношении умеренных рисков План безопасности предусматривает соразмерные меры по мониторингу, предупреждению или снижению рисков с учетом специфики инфраструктуры и изменений среды рисков.

22. В отношении низких рисков управляющий обеспечивает их периодический мониторинг и переоценку в случае изменения оперативных, технических, организационных условий или условий безопасности.

23. Если реагирование на инцидент выходит за пределы возможностей управляющего национальной критической инфраструктурой, либо инцидент нарушает или может нарушить непрерывность предоставления основной услуги или влечет системные либо межсекторальные последствия, План безопасности предусматривает по меньшей мере:

23.1. критерии и уровни эскалации инцидента;

23.2. обязанности по оценке инцидента и инициированию его эскалации;

23.3. порядок информирования ответственного органа публичной власти, Национального центра по управлению кризисами и других компетентных органов в соответствии с применимой нормативной базой;

23.4. механизмы задействования межведомственного сотрудничества и координации;

23.5. порядок включения в национальные механизмы управления кризисами собственных мер по реагированию, обеспечению непрерывности и восстановлению;

23.6. контактные данные, каналы связи и применимые схемы уведомления.

IV. РАЗРАБОТКА ПЛАНА БЕЗОПАСНОСТИ

24. Разработка Плана безопасности начинается после назначения инфраструктуры национальной критической инфраструктурой.

25. План безопасности разрабатывается и направляется на согласование в течение 9 месяцев с даты назначения инфраструктуры национальной критической инфраструктурой. Указанный срок может быть продлен не более чем на 6 месяцев с согласия Национального центра по координации защиты критических инфраструктур в

соответствии с частью (1) статьи 14 Закона № 223/2025 об идентификации, назначении и защите национальной критической инфраструктуры.

26. Внутренним решением об инициировании процесса устанавливаются по меньшей мере:

26.1. национальная критическая инфраструктура, для которой разрабатывается План безопасности;

26.2. координатор процесса разработки;

26.3. участвующие структуры и лица;

26.4. внутренний график разработки;

26.5. основные обязанности;

26.6. порядок проведения консультаций и внутреннего согласования.

27. Управляющий вправе в соответствующих случаях создать внутреннюю рабочую группу или комиссию для разработки Плана безопасности.

28. Разработка Плана безопасности включает по меньшей мере следующие этапы:

28.1. инициирование процесса разработки;

28.2. определение границ национальной критической инфраструктуры и соответствующей основной услуги;

28.3. проведение или обновление оценки рисков;

28.4. использование результатов оценки рисков;

28.5. выявление и систематизация существующих мер;

28.6. анализ соответствующих внутренних документов;

28.7. определение необходимых дополнительных мер;

28.8. определение мер по обеспечению непрерывности и восстановлению;

28.9. определение обязанностей, сроков и ресурсов;

28.10. подготовка проекта Плана безопасности;

28.11. проведение внутренних и, в соответствующих случаях, внешних консультаций;

28.12. предварительное утверждение проекта в целях его направления на согласование;

28.13. направление Плана безопасности на согласование ответственному органу публичной власти;

28.14. окончательное утверждение Плана безопасности после получения согласования;

28.15. обеспечение учета утвержденной версии Плана безопасности и введение его в действие.

29. Этапы, предусмотренные в пункте 28, осуществляются с учетом сложности национальной критической инфраструктуры и уровня выявленных рисков.

30. План безопасности в обязательном порядке разрабатывается на основании актуальной оценки рисков, результаты которой оформлены документально.

31. При разработке Плана безопасности учитываются по меньшей мере:

31.1. выявленные приоритетные риски;

31.2. соответствующие сценарии рисков;

31.3. выявленные уязвимости и зависимости;

31.4. критические функции, критические активы и основные процессы;

31.5. оцененные уровни воздействия и вероятности;

31.6. существующие меры и выявленные недостатки;

31.7. в соответствующих случаях - соответствующие документы национального уровня, касающиеся непрерывности жизненно важных функций государства, национальной устойчивости и управления кризисами.

32. При отсутствии актуальной оценки рисков либо если имеющаяся оценка более не соответствует фактической ситуации, План безопасности не может считаться разработанным надлежащим образом.

33. При разработке Плана безопасности управляющий в соответствующих случаях учитывает имеющиеся внутренние документы, относящиеся к:

33.1. обеспечению непрерывности деятельности;

33.2. реагированию на инциденты;

33.3. физической защите;

33.4. информационной и кибербезопасности;

33.5. чрезвычайным ситуациям, гражданской защите или противопожарной защите;

33.6. техническому обслуживанию и техническому восстановлению;

33.7. внутренним и внешним коммуникациям;

33.8. другим соответствующим областям.

34. Использование документов, предусмотренных в пункте 33, не освобождает от обязанности обеспечить согласованность, целостность и полноту Плана безопасности.

35. Если имеющиеся документы полностью или частично охватывают требования к Плану безопасности, управляющий вправе обратиться с просьбой о признании их эквивалентными в соответствии с Методологическими нормами, предусмотренными в приложении № 4.

V. ВНУТРЕННИЕ КОНСУЛЬТАЦИИ И ПРОВЕРКА

36. По проекту Плана безопасности проводятся внутренние консультации с соответствующими структурными подразделениями и лицами управляющего.

37. В ходе внутренних консультаций проверяются по меньшей мере:

37.1. правильность описания национальной критической инфраструктуры и основной услуги;

37.2. соответствие оценке рисков;

37.3. полнота предусмотренных мер;

37.4. реалистичность сроков и ресурсов;

37.5. четкость распределения ответственности;

37.6. согласованность с другими соответствующими внутренними документами;

37.7. соблюдение типовой структуры, предусмотренной в приложении № 3.

38. При необходимости управляющий может проводить консультации с соответствующими внешними субъектами в пределах установленных законом полномочий и с соблюдением режима защиты информации, если это необходимо для дополнения или подтверждения отдельных мер, касающихся:

38.1. взаимозависимостей;

38.2. непрерывности услуг;

38.3. обеспечения критически важными ресурсами;

38.4. реагирования и межведомственной координации;

38.5. технической или договорной поддержки, необходимой для функционирования национальной критической инфраструктуры.

39. Проведение внешних консультаций не допускает разглашения чувствительной информации, конфиденциальной информации или информации, отнесенной к государственной тайне, кроме как в случаях и на условиях, предусмотренных применимым законодательством.

VI. НАПРАВЛЕНИЕ ПЛАНА БЕЗОПАСНОСТИ

НА СОГЛАСОВАНИЕ

40. После предварительного внутреннего утверждения управляющий национальной критической инфраструктурой направляет План безопасности на согласование ответственному органу публичной власти соответствующего сектора или подсектора.

41. Пакет документов, направляемый на согласование, включает:

41.1. заявление о согласовании;

41.2. План безопасности, предварительно утвержденный на внутреннем уровне;

41.3. отчет об оценке рисков или его краткое изложение;

41.4. реестр рисков;

41.5. перечень приоритетных мер;

41.6. таблицу соответствия типовой структуре, предусмотренной в приложении № 3;

41.7. перечень документов, прилагаемых к Плану безопасности или относящихся к нему;

41.8. контактные данные офицера связи;

41.9. внутренний акт об инициировании разработки Плана безопасности или о его предварительном утверждении;

41.10. иные документы, запрошенные ответственным органом публичной власти с учетом специфики сектора.

42. План безопасности и относящиеся к нему документы передаются в установленном формате и с использованием средств передачи, предусмотренных техническими требованиями и типовыми формами, утвержденными НЦКЗКИ. Ответственный орган публичной власти может устанавливать дополнительные требования, обусловленные спецификой сектора или подсектора, с соблюдением единых требований и режима защиты чувствительной информации, конфиденциальной информации или информации, отнесенной к государственной тайне.

43. Если План безопасности содержит информацию, отнесенную к государственной тайне, или иные категории охраняемой законом информации, его

передача, предоставление доступа к нему и хранение осуществляются в соответствии с правовым режимом, применимым к такой информации.

VII. РАССМОТРЕНИЕ И СОГЛАСОВАНИЕ ПЛАНА БЕЗОПАСНОСТИ

44. Ответственный орган публичной власти рассматривает План безопасности с учетом:

44.1. соблюдения типовой структуры, предусмотренной в приложении № 3;

44.2. наличия и качества оценки рисков;

44.3. согласованности предлагаемых мер с выявленными рисками;

44.4. соразмерности мер уровню риска;

44.5. включения мер в отношении высоких и критических рисков;

44.6. четкости определения ответственности, сроков и ресурсов;

44.7. наличия процедур реагирования, обеспечения непрерывности и восстановления;

44.8. соответствия применимым отраслевым требованиям;

44.9. наличия механизмов обучения, тестирования, отчетности и обновления;

44.10. соблюдения режима защиты информации.

45. Ответственный орган публичной власти проверяет полноту пакета документов в срок, не превышающий
10 рабочих дней с даты его получения.

46. Если пакет документов является полным, ответственный орган публичной власти уведомляет об этом управляющего и рассматривает План безопасности в срок, не превышающий 30 рабочих дней с даты признания пакета документов полным.

47. Если пакет документов неполный, ответственный орган публичной власти запрашивает у управляющего недостающую информацию или документы и указывает, какие сведения или документы необходимо дополнить либо исправить.

48. Управляющий представляет запрошенные дополнения в течение 14 рабочих дней с даты получения запроса, если ответственный орган публичной власти не установит иной обоснованный срок.

49. Срок проверки полноты пакета документов исчисляется заново со дня получения запрошенных дополнений.

50. Если управляющий не представляет запрошенные дополнения в срок,

предусмотренный пунктом 48, и до его истечения не обращается с обоснованным ходатайством о продлении срока, ответственный орган публичной власти возвращает пакет документов без завершения процедуры согласования. Для возобновления процедуры представляется полный пакет документов.

51. В ходе рассмотрения по существу ответственный орган публичной власти может запросить разъяснения или дополнительную информацию, необходимые для оценки Плана безопасности.

52. Течение срока рассмотрения по существу приостанавливается со дня направления запроса, предусмотренного пунктом 51, до дня получения запрошенных разъяснений или информации. Управляющий представляет разъяснения или дополнительную информацию в течение 10 рабочих дней с даты получения запроса. Срок приостановления рассмотрения по существу не может превышать 15 рабочих дней.

53. По результатам рассмотрения ответственный орган публичной власти принимает одно из следующих решений:

53.1. о согласовании Плана безопасности;

53.2. о согласовании Плана безопасности при условии выполнения указанных мер или внесения необходимых дополнений;

53.3. о возврате Плана безопасности для пересмотра с указанием причин.

54. План безопасности может быть согласован при условии устранения выявленных несоответствий, если он в целом соответствует установленным требованиям, а такие несоответствия не влияют на применимость основных мер безопасности, обеспечения непрерывности, реагирования и восстановления.

55. В этом случае управляющий представляет ответственному органу публичной власти подтверждение устранения выявленных несоответствий в срок, установленный в заключении.

56. План безопасности возвращается для пересмотра, если выявленные недостатки или несоответствия существенно влияют на качество оценки рисков, соразмерность мер, применимость Плана либо его способность обеспечивать защиту и непрерывность основной услуги.

57. Решения, предусмотренные пунктом 53, оформляются письменным заключением, которое содержит по меньшей мере:

57.1. идентификационные данные управляющего и национальной критической инфраструктуры;

57.2. основание для рассмотрения;

57.3. рассмотренные документы;

57.4. вывод по результатам рассмотрения и принятое решение;

57.5. выявленные несоответствия, установленные условия, рекомендации или меры по устранению недостатков, в зависимости от обстоятельств;

57.6. срок устранения недостатков или повторного представления пересмотренного Плана безопасности, в зависимости от обстоятельств;

57.7. дату выдачи;

57.8. подпись уполномоченного лица.

58. В случае возврата Плана безопасности для пересмотра управляющий пересматривает его и повторно представляет ответственному органу публичной власти в течение 30 рабочих дней с даты получения заключения, если в заключении не установлен иной срок, обусловленный сложностью необходимых изменений.

59. Ответственный орган публичной власти рассматривает пересмотренный План безопасности в срок, не превышающий 30 рабочих дней с даты признания пакета документов полным, и принимает одно из решений, предусмотренных пунктом 53.

60. Срок рассмотрения по существу может быть продлен один раз не более чем на 15 рабочих дней, если это обусловлено сложностью документации, наличием информации, отнесенной к государственной тайне, либо необходимостью проведения дополнительных проверок. О продлении срока управляющий уведомляется в письменной форме до истечения первоначально установленного срока с указанием причин продления.

61. Ответственный орган публичной власти ведет учет рассмотренных планов безопасности и выданных заключений по национальным критическим инфраструктурам соответствующего сектора или подсектора.

VIII. ОКОНЧАТЕЛЬНОЕ УТВЕРЖДЕНИЕ ПЛАНА БЕЗОПАСНОСТИ

62. План безопасности окончательно утверждается руководителем управляющего национальной критической инфраструктурой либо компетентным лицом, назначенным в соответствии с применимыми внутренними актами, после его согласования с ответственным органом публичной власти.

63. Если План безопасности согласован при условии выполнения определенных требований, он может быть окончательно утвержден с обязательством реализовать меры, указанные в заключении, в сроки, установленные ответственным органом публичной власти.

64. При окончательном утверждении Плана безопасности руководство управляющего подтверждает:

64.1. принятие содержания Плана безопасности;

64.2. принятие предусмотренных мер и ответственности;

64.3. принятие обязательства по внедрению, мониторингу, тестированию и обновлению Плана безопасности;

64.4. обеспечение необходимых ресурсов в пределах своих полномочий и институциональных возможностей.

65. В окончательно утвержденном Плане безопасности указываются по меньшей мере:

65.1. дата утверждения;

65.2. подпись компетентного лица;

65.3. номер или код версии;

65.4. отметка о введении в действие;

65.5. режим доступа к документу в соответствии с применимым законодательством.

66. План безопасности вводится в действие со дня его окончательного утверждения либо с даты, указанной в нем.

67. Управляющий в течение 5 рабочих дней со дня утверждения направляет ответственному органу публичной власти копию внутреннего акта об окончательном утверждении Плана безопасности.

68. Ответственный орган публичной власти может направлять НЦКЗКИ сводную информацию о согласованных планах безопасности без разглашения чувствительной информации, конфиденциальной информации или информации, отнесенной к государственной тайне, если иное не предусмотрено применимым законодательством.

IX. РЕАЛИЗАЦИЯ И МОНИТОРИНГ ПЛАНА БЕЗОПАСНОСТИ

69. После окончательного утверждения управляющий национальной критической инфраструктурой обеспечивает реализацию мер, предусмотренных Планом безопасности, в соответствии с установленными обязанностями и сроками.

70. Реализация Плана безопасности включает, в зависимости от обстоятельств:

70.1. внутреннее информирование о возложенных обязанностях;

70.2. выделение необходимых ресурсов;

70.3. начало реализации предусмотренных мер;

70.4. включение мер в текущую деятельность соответствующих структур;

70.5. планирование обучения, тестирования и учений;

70.6. мониторинг выполнения мер;

70.7. внутреннюю отчетность о ходе реализации.

71. Меры, направленные на обработку высоких или критических рисков, реализуются и контролируются в приоритетном порядке.

72. Для мер, требующих инвестиций, закупок, выполнения работ, заключения договоров или дополнительных ресурсов, управляющий устанавливает график реализации, определяет имеющиеся источники финансирования, внутреннее распределение ответственности и, при необходимости, временные или компенсирующие меры.

73. Если отдельные необходимые меры не могут быть реализованы незамедлительно, управляющий предусматривает:

73.1. временные или компенсирующие решения;

73.2. очередность их реализации;

73.3. соответствующие обязанности и сроки;

73.4. обоснование невозможности их незамедлительной реализации;

73.5. остаточный риск, временно принимаемый управляющим.

74. Офицер связи на оперативном уровне осуществляет контроль за реализацией Плана безопасности и информирует руководство управляющего о ходе его реализации, выявленных несоответствиях и необходимости принятия дополнительных мер.

75. Управляющий информирует ответственный орган публичной власти о существенных затруднениях, которые могут повлиять на реализацию мер, предусмотренных в отношении высоких или критических рисков.

76. Ответственный орган публичной власти в пределах установленных законом полномочий осуществляет мониторинг реализации мер, предусмотренных Планами безопасности управляющих национальной критической инфраструктурой соответствующего сектора или подсектора.

X. ТЕСТИРОВАНИЕ ПЛАНА БЕЗОПАСНОСТИ

77. Управляющий обеспечивает тестирование Плана безопасности посредством проведения учений, моделирования, функциональных проверок или в иных формах, соответствующих специфике инфраструктуры и оцененным рискам.

78. Тестирование Плана безопасности проводится не реже одного раза в 2 года, а также при возникновении существенных изменений, касающихся национальной критической инфраструктуры, основной услуги, рисков, процедур, ответственности или

ресурсов, предусмотренных Планом, либо после соответствующего инцидента.

79. Тестирование Плана безопасности проводится в целях проверки применимости мер, четкости распределения ответственности, работоспособности процедур реагирования, обеспечения непрерывности и восстановления, а также выявления уязвимостей или несоответствий.

80. Тестирование может проводиться посредством:

80.1. штабных учений (*tabletop*);

80.2. функциональных учений;

80.3. оперативных учений;

80.4. технического моделирования;

80.5. проверки каналов связи и оповещения;

80.6. тестирования процедур обеспечения непрерывности и восстановления;

80.7. иных форм тестирования, соответствующих специфике инфраструктуры.

81. Учения, предусматривающие сценарии со значительным воздействием на основные услуги, системными или межсекторальными последствиями, проводятся при необходимости с участием компетентных органов Национальной системы управления кризисами в целях проверки механизмов оповещения, сотрудничества и межведомственной координации.

82. Результаты тестирования оформляются отчетом о тестировании или проведенных учениях, который содержит по меньшей мере:

82.1. цели тестирования;

82.2. использованный сценарий;

82.3. участников;

82.4. протестированные процедуры;

82.5. установленные факты;

82.6. выявленные несоответствия или уязвимости;

82.7. корректирующие меры;

82.8. ответственных лиц и сроки;

82.9. выводы и извлеченные уроки.

83. Установленные факты, выводы и извлеченные уроки по результатам

тестирования Плана безопасности, управления кризисными ситуациями, национальных учений и крупных инцидентов подлежат обязательному анализу и учету при обновлении оценки рисков и, при необходимости, при пересмотре и обновлении Плана безопасности в соответствии с приложением № 5.

XI. УЧЕТ ВЕРСИЙ И ОТСЛЕЖИВАЕМОСТЬ ИЗМЕНЕНИЙ

84. Управляющий обеспечивает учет всех версий Плана безопасности.

85. Учет версий включает по меньшей мере:

85.1. номер или код версии;

85.2. дату разработки;

85.3. дату согласования;

85.4. дату окончательного утверждения;

85.5. описание внесенных изменений;

85.6. основание для внесения изменений;

85.7. ответственных лиц или структурные подразделения;

85.8. режим доступа к документу.

86. Управляющий обеспечивает хранение действующей и предыдущих версий Плана безопасности в соответствии с правовым режимом, применимым к документу.

87. Каждая новая версия Плана безопасности или каждое существенное обновление подлежат регистрации во внутренней системе учета документов, относящихся к национальной критической инфраструктуре.

88. Соответствующие структурные подразделения управляющего информируются о действующей версии Плана безопасности в пределах своих полномочий и с учетом необходимости работы с содержащейся в нем информацией.

XII. ЗАЩИТА ИНФОРМАЦИИ

89. План безопасности и относящиеся к нему документы обрабатываются с соблюдением правового режима, применимого к информации, отнесенной к государственной тайне, персональным данным, чувствительной информации о национальных критических инфраструктурах и иным категориям охраняемой законом информации.

90. Доступ к Плану безопасности и относящимся к нему документам предоставляется только лицам, непосредственно выполняющим соответствующие обязанности и обосновавшим необходимость работы с такой информацией, с соблюдением правового режима, применимого к чувствительной информации,

конфиденциальной информации, информации, отнесенной к государственной тайне, и иным категориям охраняемой законом информации.

91. Управляющий устанавливает внутренние меры по учету, хранению, предоставлению доступа, копированию, передаче, архивированию и защите Плана безопасности и связанных с ним документов.

92. Информация об уязвимостях, сценариях риска, мерах безопасности, возможностях реагирования, уязвимых элементах и критических взаимозависимостях защищается сообразно уровню риска, возникающего в случае ее разглашения.

93. Передача Плана безопасности ответственному органу публичной власти или иным уполномоченным субъектам осуществляется с использованием средств, обеспечивающих надлежащую защиту информации в соответствии с применимым правовым режимом.

XIII. ОБЩИЕ ПРАВИЛА ПРИМЕНЕНИЯ

И МЕТОДОЛОГИЧЕСКОГО СОГЛАСОВАНИЯ

94. План безопасности согласуется с оценкой рисков, планами обеспечения непрерывности, планами физической защиты, планами гражданской защиты, планами кибербезопасности, планами реагирования, оперативными процедурами и другими соответствующими документами управляющего, а также, при необходимости, с национальными документами, касающимися непрерывности жизненно важных функций государства, национальной устойчивости и управления кризисами.

95. В отношении национальных критических инфраструктур, имеющих существенные взаимозависимости с другими субъектами, управляющий обеспечивает включение в План безопасности необходимых механизмов координации и сотрудничества.

96. Разработка и утверждение Плана безопасности не освобождают управляющего от обязанности соблюдать иные правовые, отраслевые, технические и процедурные требования, применимые к национальной критической инфраструктуре.

97. Если План безопасности требует внесения изменений в связи с обновлением оценки рисков, возникновением инцидента, проведением учений, изменением инфраструктуры или среды риска, управляющий инициирует его пересмотр в соответствии с приложением № 5.

98. Ответственные органы публичной власти могут разрабатывать отраслевые инструкции и типовые формы документов для применения настоящих Методологических норм в соответствующих секторах и подсекторах, уведомляя об этом НЦКЗКИ.

99. Разработка, передача, рассмотрение, согласование, утверждение и хранение Плана безопасности национальных критических инфраструктур в области обороны, общественного порядка и государственной безопасности осуществляются с

соблюдением правового режима, применимого к информации, отнесенной к государственной тайне, чувствительной информации о национальных критических инфраструктурах и иным категориям охраняемой законом информации. Доступ к Плану безопасности и относящимся к нему документам предоставляется только уполномоченным лицам с использованием средств, соответствующих правовому режиму, применимому к такой информации.

100. НЦКЗКИ разрабатывает и предоставляет ответственным органам публичной власти и управляющим национальной критической инфраструктурой типовые формы и стандартизированные методологические инструменты для применения настоящих Методологических норм, включая типовые формы Плана безопасности, образцы таблиц соответствия, типовые формы отчетности, образцы документов для согласования и пересмотра, а также иные инструменты, необходимые для единообразного применения процедуры разработки, согласования, утверждения, реализации, тестирования, пересмотра и обновления Плана безопасности.

Приложение № 3

к Постановлению Правительства

№ 483/2026

ТИПОВАЯ СТРУКТУРА

Плана безопасности управляющего национальной

критической инфраструктурой

Раздел 1

Общие сведения

1. Глава, посвященная общим сведениям, должна содержать по меньшей мере:

1.1. полное наименование управляющего национальной критической инфраструктурой (в дальнейшем – *управляющий*);

1.2. организационно-правовую форму;

1.3. местонахождение и контактные данные;

1.4. наименование национальной критической инфраструктуры;

1.5. сектор и подсектор, к которым она относится;

1.6. правовое основание назначения инфраструктуры в качестве национальной критической инфраструктуры;

1.7. версию Плана безопасности управляющего национальной критической инфраструктурой (в дальнейшем – *План безопасности*), дату его разработки и дату

утверждения;

1.8. уровень доступа к документу, режим его хранения и порядок обращения с ним;

1.9. сведения о лицах, ответственных за разработку, обновление и хранение Плана безопасности;

1.10. контактные данные офицера связи по безопасности национальной критической инфраструктуры.

Раздел 2

Цель, задачи и область применения плана безопасности

2. Глава, посвященная цели, задачам и области применения, должна содержать по меньшей мере:

2.1. цель Плана безопасности;

2.2. общие и конкретные задачи в области безопасности;

2.3. область применения Плана безопасности;

2.4. сведения о национальной критической инфраструктуре, услугах, процессах, местах размещения и структурах, на которые распространяется План безопасности;

2.5. пределы применения Плана безопасности;

2.6. взаимосвязь Плана безопасности с другими планами, процедурами и внутренними или отраслевыми документами;

2.7. исходные допущения, принятые при разработке Плана безопасности.

3. Задачи Плана безопасности должны быть направлены по меньшей мере на:

3.1. предотвращение и снижение приоритетных рисков;

3.2. защиту критических функций, критических активов и основных процессов;

3.3. поддержание или возобновление предоставления основной услуги на минимально приемлемом уровне;

3.4. обеспечение скоординированного реагирования в случае инцидентов;

3.5. восстановление национальной критической инфраструктуры и возобновление ее функционирования;

3.6. защиту чувствительной информации, конфиденциальной информации или информации, отнесенной к государственной тайне;

3.7. сотрудничество с ответственными органами публичной власти и другими соответствующими субъектами;

3.8. сохранение вклада национальной критической инфраструктуры в обеспечение непрерывности жизненно важных функций государства и укрепление национальной устойчивости.

Раздел 3

Описание национальной критической

инфраструктуры и основной услуги

4. Глава, посвященная описанию национальной критической инфраструктуры и основной услуги, должна содержать по меньшей мере:

4.1. общее описание национальной критической инфраструктуры;

4.2. ее местонахождение, места размещения и основные компоненты;

4.3. описание предоставляемой основной услуги;

4.4. значение инфраструктуры для обеспечения непрерывности предоставления основной услуги;

4.5. основные операционные процессы и функциональные потоки;

4.6. минимальные допустимые параметры функционирования;

4.7. условия, при которых непрерывность предоставления основной услуги считается нарушенной;

4.8. максимально допустимую продолжительность перерыва в предоставлении основной услуги, если она установлена;

4.9. минимально приемлемый уровень функционирования в режиме ограниченной работоспособности;

4.10. значение результатов оценки рисков для определения мер безопасности, обеспечения непрерывности деятельности, реагирования и восстановления, в том числе с учетом потенциального воздействия нарушения функционирования национальной критической инфраструктуры на непрерывность жизненно важных функций государства, а также связанных с таким нарушением системных или межсекторальных последствий.

Раздел 4

Критические функции, критические активы,

основные процессы и другие важные элементы

5. Глава, посвященная критическим функциям, критическим активам, основным процессам и другим элементам, имеющим важное значение для предоставления основной услуги, должна содержать по меньшей мере:

5.1. идентификацию критических функций;

5.2. идентификацию критических активов;

5.3. идентификацию основных процессов;

5.4. идентификацию других элементов, имеющих важное значение для поддержания или возобновления предоставления основной услуги;

5.5. ключевой персонал и необходимые компетенции;

5.6. критические ресурсы, необходимые для функционирования;

5.7. приоритетность критических функций, критических активов и основных процессов;

5.8. влияние их недоступности на предоставление основной услуги.

Раздел 5

Зависимости и взаимозависимости

6. Глава, посвященная зависимостям и взаимозависимостям, должна содержать по меньшей мере:

6.1. внутренние зависимости между функциями, процессами, системами и компонентами;

6.2. внешние зависимости от поставщиков товаров, поставщиков услуг, операторов и партнеров;

6.3. зависимости от энергоснабжения, водоснабжения, связи, информационных систем, транспорта или других критических ресурсов;

6.4. взаимозависимости с другими критическими инфраструктурами или основными услугами;

6.5. уязвимости, обусловленные этими зависимостями;

6.6. возможные цепные или каскадные эффекты;

6.7. меры по снижению критических зависимостей, в зависимости от обстоятельств;

6.8. механизмы координации с субъектами, от которых зависит функционирование национальной критической инфраструктуры.

Раздел 6

Результаты оценки рисков

7. Глава, посвященная результатам оценки рисков, должна содержать по меньшей мере:

7.1. краткое изложение результатов проведенной оценки рисков;

7.2. выявленные риски, сгруппированные по категориям;

7.3. соответствующие сценарии риска;

7.4. выявленные уязвимости;

7.5. оценку воздействия и вероятности;

7.6. баллы и уровни риска;

7.7. приоритетные риски;

7.8. остаточные риски, в зависимости от обстоятельств;

7.9. основные выводы по результатам оценки;

7.10. значение результатов оценки рисков для определения мер безопасности, обеспечения непрерывности деятельности, реагирования и восстановления.

8. К Плану безопасности прилагаются карточки оценки рисков, реестр рисков, матрица рисков и соответствующие подтверждающие документы с соблюдением применимого режима доступа.

Раздел 7

Действующие меры безопасности

9. Глава, посвященная действующим мерам безопасности, должна содержать описание по меньшей мере:

9.1. мер физической защиты;

9.2. технических и технологических мер защиты;

9.3. организационных и процедурных мер;

9.4. мер информационной безопасности и кибербезопасности;

9.5. мер по контролю доступа;

9.6. мер по обеспечению безопасности персонала;

9.7. мер по обнаружению, оповещению и первичному реагированию;

9.8. мер по мониторингу инцидентов и представлению сообщений о них;

9.9. мер по защите информации;

9.10. мер по резервированию и обеспечению альтернативного функционирования, в зависимости от обстоятельств.

10. Действующие меры описываются с указанием соответствующих рисков и уязвимостей, а также критических функций, критических активов или основных процессов, защиту которых они обеспечивают.

Раздел 8

Дополнительные меры и план реализации

11. Глава, посвященная дополнительным мерам и плану реализации, должна содержать меры, необходимые для обработки приоритетных рисков и устранения выявленных уязвимостей.

12. В отношении каждого приоритетного риска План безопасности должен предусматривать по меньшей мере:

12.1. необходимые дополнительные меры;

12.2. цель каждой меры;

12.3. вид меры: организационная, техническая, процедурная или физическая мера, мера кибербезопасности, обеспечения непрерывности деятельности, реагирования или восстановления либо мера иного соответствующего вида;

12.4. уровень приоритетности;

12.5. лицо, ответственное за реализацию;

12.6. необходимые ресурсы;

12.7. срок реализации;

12.8. показатели выполнения;

12.9. способ проверки;

12.10. принятый остаточный риск, в зависимости от обстоятельств.

13. Дополнительные меры определяются с учетом уровня риска, срочности их принятия, фактических возможностей управляющего по их реализации и необходимости обеспечения непрерывности предоставления основной услуги.

14. Дополнительные меры, как правило, представляются в таблице реализации, содержащей по меньшей мере следующие графы:

№ п/п	Риск, на который направлена мера	Предлагаемая мера	Вид меры	Ответственное лицо	Срок	Необходимые ресурсы	Показатель выполнения	Статус выполнения

Раздел 9

Меры по обеспечению непрерывности деятельности

15. Глава, посвященная обеспечению непрерывности деятельности, должна содержать по меньшей мере:

15.1. меры по поддержанию критических функций;

15.2. решения для функционирования в режиме ограниченной работоспособности, а также альтернативного или резервного функционирования;

15.3. приоритеты поддержания и возобновления предоставления основной услуги;

15.4. минимальные ресурсы, необходимые для обеспечения непрерывности деятельности;

15.5. процедуры активации мер по обеспечению непрерывности деятельности;

15.6. обязанности задействованных структур и лиц;

15.7. механизмы внутренней и внешней координации;

15.8. максимально допустимую продолжительность перерыва в функционировании, если она установлена;

15.9. целевые сроки возобновления критических функций, в зависимости от обстоятельств;

15.10. решения по замещению, перемещению, резервированию или организации альтернативного функционирования.

Раздел 10

Меры реагирования, уведомления и восстановления

16. Глава, посвященная реагированию, уведомлению и восстановлению, должна содержать по меньшей мере:

16.1. меры реагирования при возникновении инцидента;

16.2. процедуры оповещения, информирования и эскалации;

16.3. меры по ограничению последствий;

16.4. меры по поэтапному или полному восстановлению функционирования;

16.5. приоритеты восстановления;

16.6. ресурсы, необходимые для восстановления;

16.7. порядок документирования инцидентов и использования извлеченных уроков;

16.8. порядок внутреннего уведомления руководства управляющего;

16.9. порядок уведомления ответственного органа публичной власти;

16.10. порядок уведомления Национального центра по координации защиты критических инфраструктур (в дальнейшем – *НЦКЗКИ*), в зависимости от обстоятельств;

16.11. порядок уведомления других компетентных органов или соответствующих субъектов согласно применимому законодательству;

16.12. лиц или структуры, ответственные за управление инцидентами;

16.13. критерии и уровни эскалации инцидентов, которые превышают возможности управляющего по реагированию либо вызывают системные или межсекторальные последствия;

16.14. критерии и порядок информирования Национального центра по управлению кризисами согласно применимой нормативной базе;

16.15. механизмы активации межведомственной координации в рамках Национальной системы управления кризисами;

16.16. порядок включения в национальные механизмы управления кризисными ситуациями предусмотренных Планом безопасности мер реагирования, мер по обеспечению непрерывности деятельности и мер по восстановлению.

17. Процедуры реагирования и восстановления должны согласовываться с соответствующими сценариями риска и мерами по обеспечению непрерывности деятельности, предусмотренными Планом безопасности.

Раздел 11

Организация, обязанности и механизмы координации

18. Глава, посвященная организации, обязанностям и механизмам координации, должна содержать по меньшей мере:

18.1. внутренние структуры, участвующие в применении Плана безопасности;

18.2. полномочия руководства управляющего;

18.3. полномочия офицера связи;

18.4. полномочия операционных, технических, административных и вспомогательных структур;

18.5. механизмы внутренней координации;

18.6. механизмы сотрудничества с ответственными органами публичной власти, компетентными органами и другими соответствующими субъектами;

18.7. механизмы координации с поставщиками товаров, поставщиками услуг и критически важными партнерами;

18.8. процедуры передачи принятия решений на более высокий уровень в случае нарушения функционирования или возникновения инцидента;

18.9. механизмы сотрудничества и координации с Национальным центром по управлению кризисами и другими компетентными органами в случае инцидентов, имеющих системные или межсекторальные последствия.

Раздел 12

Коммуникация, отчетность и обмен информацией

19. Глава, посвященная коммуникации, отчетности и обмену информацией, должна содержать по меньшей мере:

19.1. механизмы внутренней коммуникации;

19.2. механизмы коммуникации с ответственным органом публичной власти;

19.3. механизмы коммуникации с НЦКЗКИ, в зависимости от обстоятельств;

19.4. механизмы коммуникации с другими компетентными органами;

19.5. порядок коммуникации с поставщиками товаров, поставщиками услуг, партнерами и другими соответствующими субъектами;

19.6. лиц, уполномоченных передавать информацию;

19.7. правила публичного информирования и кризисной коммуникации, включая их согласование, в зависимости от обстоятельств, с национальными механизмами коммуникации в кризисных ситуациях для обеспечения согласованности и единства официальных сообщений;

19.8. процедуры представления сообщений об инцидентах, нарушениях функционирования и соответствующих уязвимостях;

19.9. механизмы обмена информацией о рисках, угрозах, уязвимостях и мерах безопасности.

20. Публичное информирование об инцидентах, затрагивающих национальную критическую инфраструктуру, осуществляется исключительно лицами, назначенными или уполномоченными для этой цели управляющим национальной критической инфраструктурой либо, в зависимости от обстоятельств, ответственным органом публичной власти или НЦКЗКИ, в пределах установленных законом полномочий и с соблюдением механизмов межведомственной координации, применимого законодательства и требований к защите информации, а также с учетом необходимости не допустить паники, дезинформации или создания дополнительных угроз безопасности национальной критической инфраструктуры.

Раздел 13

Обучение, тестирование и учения

21. Глава, посвященная обучению, тестированию и учениям, должна содержать по меньшей мере:

21.1. программу обучения соответствующего персонала;

21.2. обучение офицера связи и ключевого персонала;

21.3. виды запланированных тестов и учений;

21.4. периодичность проведения тестов и учений;

21.5. соответствующие сценарии тестирования, включая, в зависимости от обстоятельств, сценарии межсекторальных кризисных ситуаций;

21.6. порядок оценки результатов;

21.7. меры по устранению выявленных недостатков;

21.8. сведения о проведенном обучении, тестах и учениях;

21.9. порядок проверки взаимодействия и координации между управляющим национальной критической инфраструктурой, другими соответствующими управляющими и компетентными органами в рамках Национальной системы управления кризисами.

Раздел 14

Пересмотр и обновление Плана безопасности

22. Глава, посвященная пересмотру и обновлению Плана безопасности, должна содержать по меньшей мере:

22.1. периодичность пересмотра Плана безопасности;

22.2. случаи, требующие внеочередного пересмотра;

22.3. лиц и структуры, ответственные за обновление;

22.4. порядок утверждения изменений;

22.5. учет версий и изменений;

22.6. порядок отражения в Плане безопасности изменений, обусловленных обновлением оценки рисков;

22.7. порядок информирования соответствующих внутренних структур о внесенных изменениях;

22.8. механизм изъятия из обращения или передачи на архивное хранение устаревших версий.

Раздел 15

Режим документа, хранение и обращение с информацией

23. Глава, посвященная режиму документа, должна содержать по меньшей мере:

23.1. уровень доступа и режим конфиденциальности;

23.2. перечень лиц, уполномоченных знакомиться с Планом безопасности, использовать его и вносить в него изменения;

23.3. правила хранения, архивирования и тиражирования;

23.4. порядок внутренней и внешней передачи;

23.5. порядок защиты чувствительной информации, конфиденциальной информации или информации, отнесенной к государственной тайне, в зависимости от обстоятельств;

23.6. учет распространения Плана безопасности;

23.7. перечень лиц или структур, имеющих доступ к Плану безопасности;

23.8. лицо, ответственное за хранение официальной версии;

23.9. меры по изъятию из обращения утративших актуальность версий.

Раздел 16

Приложения к Плану безопасности

24. К Плану безопасности в зависимости от обстоятельств прилагаются:

24.1. карточки оценки рисков;

24.2. реестр рисков;

24.3. матрица рисков;

24.4. схемы, карты, планы размещения и функциональные диаграммы;

24.5. списки оперативных контактов;

24.6. реестры критических активов и основных ресурсов;

24.7. соответствующие операционные процедуры;

24.8. связанные с Планом безопасности планы или выписки из них;

24.9. таблица дополнительных мер с указанием плана их реализации;

24.10. сведения о проведенном обучении, тестах и учениях;

24.11. записки об обновлении и учет внесенных изменений;

24.12. перечень лиц или структур, имеющих доступ к Плану безопасности;

24.13. учет распространения Плана безопасности;

24.14. иные необходимые обосновывающие документы.

Раздел 17

Минимальные требования к форме

и содержанию

25. План безопасности должен быть изложен ясно и последовательно и структурирован таким образом, чтобы обеспечить возможность его эффективного применения в нормальных условиях и при нарушениях функционирования.

26. Включенная в План безопасности информация должна быть актуальной, проверяемой, взаимосогласованной и соответствовать результатам оценки рисков.

27. План безопасности не может носить исключительно описательный или декларативный характер и должен содержать конкретные меры, сведения об ответственных лицах, сроках, ресурсах и показателях, а также механизмы его применения.

28. Отсутствие одного или нескольких предусмотренных настоящим приложением существенных элементов влечет необходимость дополнения Плана безопасности либо, в зависимости от обстоятельств, невозможность его согласования или признания его эквивалентности.

29. Если определенная информация неприменима к оцениваемой национальной критической инфраструктуре, управляющий прямо указывает на это и обосновывает ее неприменимость.

30. План безопасности составляется в письменной форме и хранится в условиях, обеспечивающих защиту содержащейся в нем информации.

Приложение № 4

к Постановлению Правительства

№ 483/2026

МЕТОДОЛОГИЧЕСКИЕ НОРМЫ

признания существующих документов эквивалентными плану безопасности управляющего национальной критической инфраструктурой

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Методологические нормы устанавливают правила и процедуры, посредством которых определяется, что существующий документ или совокупность существующих документов, разработанных управляющим национальной критической инфраструктурой (в дальнейшем – *управляющий*), полностью либо в достаточной степени охватывают минимальные требования, предъявляемые к Плану безопасности управляющего национальной критической инфраструктурой (в дальнейшем – *План безопасности*).

2. Настоящие Методологические нормы направлены на недопущение необоснованного дублирования уже существующих внутренних документов при условии, что они являются релевантными, актуальными, применимыми и соответствуют требованиям настоящего постановления.

3. Признание документов эквивалентными не осуществляется автоматически и не может быть обусловлено лишь наличием ранее разработанного внутреннего документа независимо от его наименования.

4. Возможность признания документа или совокупности документов эквивалентными оценивается исходя из их фактического содержания, а не только из их наименования.

5. Признание документов эквивалентными не освобождает управляющего от обязанности обеспечивать полноту, актуальность, применимость и проверяемость таких документов.

6. Таблица соответствия существующих документов Плану безопасности используется для проверки соответствия существующих документов типовой структуре Плана безопасности, предусмотренной приложением № 3.

7. Документы, признанные эквивалентными, действуют в пределах и на

условиях, установленных актом о признании их эквивалентными.

II. ДОКУМЕНТЫ, КОТОРЫЕ МОГУТ БЫТЬ ПРЕДСТАВЛЕНЫ ДЛЯ ПРИЗНАНИЯ ЭКВИВАЛЕНТНЫМИ

8. Для признания эквивалентными в зависимости от обстоятельств могут быть представлены:

8.1. планы внутренней безопасности;

8.2. планы обеспечения непрерывности деятельности;

8.3. планы реагирования на инциденты;

8.4. планы физической защиты;

8.5. планы информационной или кибербезопасности;

8.6. планы управления чрезвычайными ситуациями, гражданской защиты или противопожарной защиты;

8.7. планы антитеррористической защиты – в зависимости от обстоятельств;

8.8. планы локализации и ликвидации аварийных ситуаций, разработанные в соответствии с законодательством в области промышленной безопасности;

8.9. комплексы взаимосвязанных процедур, положений, реестров, инструкций и иных соответствующих внутренних документов;

8.10. документы по управлению рисками, обеспечению непрерывности, восстановлению и устойчивости;

8.11. иные документы, содержание которых охватывает минимальные требования, предъявляемые к Плану безопасности.

9. Признание эквивалентности может быть запрошено:

9.1. в отношении одного документа;

9.2. в отношении комплекта документов, если в совокупности они охватывают минимальные требования, предъявляемые к Плану безопасности;

9.3. в части отдельных глав, разделов или элементов Плана безопасности.

10. При признании комплекта документов эквивалентным Плану безопасности управляющий представляет сведения о взаимосвязи между документами и о том, какие элементы типовой структуры Плана безопасности, предусмотренной приложением № 3, охватывает каждый из них.

III. ОБЩИЕ УСЛОВИЯ ПРИЗНАНИЯ ЭКВИВАЛЕНТНОСТИ

11. Признание эквивалентности допускается только в том случае, если существующий документ или комплект существующих документов:

11.1. действует на дату обращения;

11.2. утвержден в установленном законом порядке компетентным органом или лицом;

11.3. применим к конкретной национальной критической инфраструктуре, для которой запрашивается признание его эквивалентности;

11.4. учитывает основную услугу, предоставляемую посредством национальной критической инфраструктуры;

11.5. содержит четкие, согласованные между собой и практически применимые положения;

11.6. основан, в зависимости от обстоятельств, на оценке рисков либо согласуется с ее результатами;

11.7. предусматривает, в зависимости от обстоятельств, конкретные меры по обеспечению безопасности, поддержанию непрерывности, реагированию или восстановлению;

11.8. устанавливает обязанности, сроки и механизмы реализации;

11.9. позволяет проверить его соответствие минимальным требованиям, предъявляемым к Плану безопасности;

11.10. может быть рассмотрен ответственным органом публичной власти с соблюдением применимого режима доступа.

12. Не может быть признан эквивалентным документ, который:

12.1. носит исключительно описательный, декларативный или общий характер;

12.2. не предусматривает конкретных мер, обязанностей и механизмов реализации;

12.3. не адаптирован к конкретной национальной критической инфраструктуре;

12.4. не учитывает основную услугу, предоставляемую посредством национальной критической инфраструктуры;

12.5. устарел, является неполным или неприменимым;

12.6. не согласован с оценкой рисков;

12.7. не позволяет проверить его соответствие минимальным требованиям, предъявляемым к Плану безопасности;

12.8. не может быть предоставлен ответственному органу публичной власти в соответствии с законом.

13. Если один или несколько элементов отсутствуют либо недостаточно проработаны, возможны:

13.1. частичное признание эквивалентности;

13.2. условное признание эквивалентности с обязательным дополнением документа или комплекта документов в установленный срок;

13.3. отказ в признании эквивалентности.

IV. МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ДОКУМЕНТОВ, ПРИЗНАВАЕМЫХ ЭКВИВАЛЕНТНЫМИ

14. Для признания полной эквивалентности существующий документ или комплект существующих документов должен охватывать по меньшей мере следующие элементы:

14.1. идентификацию управляющего, национальной критической инфраструктуры и предоставляемой основной услуги;

14.2. цель, задачи и сферу применения;

14.3. описание критических функций, критических активов, основных процессов и важных элементов;

14.4. выявление соответствующих зависимостей и взаимозависимостей;

14.5. наличие документально оформленной оценки рисков или эквивалентных ей элементов;

14.6. выявление соответствующих рисков, сценариев риска и уязвимостей;

14.7. существующие меры безопасности;

14.8. необходимые дополнительные меры и порядок их реализации;

14.9. меры по обеспечению непрерывности;

14.10. меры по реагированию, уведомлению и восстановлению;

14.11. внутреннюю организацию, обязанности и механизмы координации;

14.12. связь, отчетность и обмен информацией;

14.13. порядок участия, в зависимости от обстоятельств, национальной критической инфраструктуры в обеспечении непрерывного осуществления жизненно важных функций государства и механизмы координации с компетентными органами в

кризисных ситуациях;

14.14. обучение, тестирование и учения, в зависимости от обстоятельств;

14.15. правила пересмотра, обновления и учета изменений;

14.16. режим обращения с документом и защиту соответствующей информации.

15. Минимальные требования, предусмотренные пунктом 14, анализируются с учетом типовой структуры Плана безопасности, предусмотренной приложением № 3.

16. Если документ или комплект документов охватывает лишь часть минимальных требований, допускается частичное признание эквивалентности с обязательным дополнением документа или комплекта документов недостающими элементами.

17. В отношении элементов, которые не отражены или недостаточно раскрыты, управляющий разрабатывает дополнения, разделы, приложения, процедуры либо дополнительные документы.

V. ИНИЦИИРОВАНИЕ ПРОЦЕДУРЫ ПРИЗНАНИЯ ЭКВИВАЛЕНТНОСТИ

18. Процедура признания эквивалентности инициируется по обращению управляющего национальной критической инфраструктурой.

19. Обращение о признании эквивалентности составляется в письменной форме и подается в ответственный орган публичной власти, компетентный в соответствующем секторе или подсекторе.

20. В обращении о признании эквивалентности указываются по меньшей мере:

20.1. национальная критическая инфраструктура, для которой запрашивается признание эквивалентности;

20.2. документ или документы, представляемые для признания эквивалентными;

20.3. вид запрашиваемого признания эквивалентности: полное, частичное или условное;

20.4. обоснование обращения;

20.5. сведения об утверждении и действительности соответствующих документов;

20.6. лицо, ответственное со стороны управляющего за сопровождение процедуры признания эквивалентности;

20.7. контактные данные офицера связи по безопасности национальной критической инфраструктуры.

VI. ДОКУМЕНТЫ, НЕОБХОДИМЫЕ ДЛЯ ПРИЗНАНИЯ ЭКВИВАЛЕНТНОСТИ

21. К обращению о признании эквивалентности прилагаются по меньшей мере:

21.1. копия документа или копии документов, представляемых для признания эквивалентными;

21.2. сводная записка о признании эквивалентности;

21.3. заполненная таблица соответствия;

21.4. подтверждение того, что соответствующий документ или документы утверждены;

21.5. сведения о действующей редакции и дате последнего обновления;

21.6. отчет об оценке рисков или его краткое изложение;

21.7. перечень документов, представляемых для признания эквивалентными;

21.8. сведения о применении, тестировании или обновлении документов, в зависимости от обстоятельств;

21.9. иные соответствующие подтверждающие документы, в зависимости от обстоятельств.

22. Если запрашивается признание комплекта документов эквивалентными, управляющий дополнительно представляет:

22.1. полный перечень документов;

22.2. сведения о роли каждого документа в обеспечении соответствия типовой структуре Плана безопасности;

22.3. сведения о взаимосвязи между документами;

22.4. основной документ или сводную записку, обеспечивающие единство комплекта документов и согласованность их применения.

23. При отсутствии четкой взаимосвязи между представленными документами полное признание эквивалентности не допускается.

VII. ТАБЛИЦА СООТВЕТСТВИЯ

24. Возможность признания эквивалентности оценивается путем заполнения таблицы соответствия между типовой структурой Плана безопасности и существующим документом или комплектом существующих документов.

25. Таблица соответствия имеет следующую минимальную структуру:

№ п/п	Минимальный обязательный элемент Плана безопасности	Наличие в документе, представляемом для признания эквивалентным: Да/Нет/Частично	Наименование документа (документов) и соответствующая глава или пункт	Оценка достаточности содержания	Замечания/ необходимые дополнения
1.	Общие сведения об управляющем и национальной критической инфраструктуре				
2.	Цель, задачи и сфера применения				
3.	Описание национальной критической инфраструктуры и основной услуги				
4.	Критические функции, критические активы и основные процессы				
5.	Зависимости и взаимозависимости				
6.	Результаты оценки рисков				
7.	Сценарии риска и уязвимости				
8.	Существующие меры безопасности				
9.	Дополнительные меры и план их реализации				
10.	Меры по обеспечению непрерывности деятельности				
11.	Меры по реагированию, уведомлению и восстановлению				
12.	Организация, обязанности и механизмы координации				
13.	Связь, отчетность и обмен информацией				
14.	Обучение, тестирование и учения				
15.	Пересмотр, обновление и учет версий				
16.	Режим обращения с документом, хранение и передача информации				

26. В графе «Наличие в документе, представляемом для признания эквивалентным» указывается один из следующих вариантов:

26.1. «Да», если элемент отражен полностью;

26.2. «Частично», если элемент отражен не полностью или требует дополнений;

26.3. «Нет», если элемент не отражен.

27. В графе «Оценка достаточности содержания» в зависимости от обстоятельств указывается:

27.1. «достаточно»;

27.2. «частично достаточно»;

27.3. «недостаточно».

28. В графе «Замечания/необходимые дополнения» указываются отсутствующие элементы, несогласованности, необходимость обновления либо любые иные условия, необходимые для признания эквивалентности.

29. Таблица соответствия первоначально заполняется управляющим и проверяется ответственным органом публичной власти в ходе рассмотрения обращения о признании эквивалентности.

VIII. РАССМОТРЕНИЕ ОБРАЩЕНИЯ О ПРИЗНАНИИ ЭКВИВАЛЕНТНОСТИ

30. Возможность признания эквивалентности оценивается ответственным органом публичной власти в пределах полномочий, установленных законом.

31. В ходе анализа проверяются по меньшей мере:

31.1. релевантность документа для соответствующей национальной критической инфраструктуры;

31.2. актуальность и действительность документа;

31.3. полнота и достаточность содержания;

31.4. практический характер и применимость предусмотренных мер;

31.5. согласованность документа или комплекта документов, представляемых для признания эквивалентными, с оценкой рисков в отношении национальной критической инфраструктуры;

31.6. отражение существующих мер и оценки их эффективности;

31.7. наличие и актуальность Реестра рисков, в зависимости от обстоятельств;

31.8. наличие установленных обязанностей, сроков и механизмов реализации;

31.9. наличие правил пересмотра и обновления;

31.10. соответствие типовой структуре, предусмотренной приложением № 3;

31.11. режим защиты информации;

31.12. совместимость документа или комплекта документов, представляемых для признания эквивалентными, с национальными механизмами управления кризисами и применимыми процедурами межведомственного сотрудничества, в зависимости от обстоятельств;

31.13. возможность проверки документа и его приложений.

32. Оценка эквивалентности проводится путем заполнения и рассмотрения таблицы соответствия.

33. Ответственный орган публичной власти рассматривает обращение о признании эквивалентности в течение 14 рабочих дней со дня получения полного пакета документов.

34. В рамках процедуры признания эквивалентности у управляющего могут быть запрошены:

34.1. дополнительные разъяснения;

34.2. недостающие документы или приложения;

34.3. обновление отдельных сведений;

34.4. заполнение таблицы соответствия;

34.5. сведения о порядке практического применения документа или документов, представляемых для признания эквивалентными.

35. Течение срока рассмотрения приостанавливается со дня запроса дополнений до дня получения запрошенных сведений или документов.

36. Управляющий направляет запрошенные дополнения в течение 5 рабочих дней с даты получения запроса, если ответственным органом публичной власти не установлен иной обоснованный срок.

IX. РЕЗУЛЬТАТ ПРОЦЕДУРЫ ПРИЗНАНИЯ ЭКВИВАЛЕНТНОСТИ

37. По итогам рассмотрения процедура признания эквивалентности может завершиться:

37.1. признанием эквивалентности в полном объеме;

37.2. частичным признанием эквивалентности;

37.3. условным признанием эквивалентности;

37.4. отказом в признании эквивалентности.

38. Признание эквивалентности в полном объеме допускается, если все существенные элементы, предусмотренные настоящим постановлением и типовой структурой Плана безопасности, установлены и признаны достаточными.

39. Частичное признание эквивалентности допускается, если документ или комплект документов охватывает лишь отдельные главы, разделы либо требования Плана безопасности.

40. В случае частичного признания эквивалентности управляющий дополняет неохваченные элементы путем разработки дополнительных разделов, приложений или документов.

41. Условное признание эквивалентности допускается, если:

41.1. отдельные элементы являются частично достаточными;

41.2. отсутствуют несущественные элементы либо элементы, которые могут быть дополнены в разумный срок;

41.3. необходимо дополнение отдельных существующих документов либо установление взаимосвязи между ними;

41.4. документ или комплект документов может быть приведен в соответствие посредством четко определенных мер по устранению недостатков.

42. В случае условного признания эквивалентности прямо устанавливаются:

42.1. элементы, подлежащие дополнению, исправлению либо обновлению;

42.2. срок устранения недостатков;

42.3. документы или подтверждающие материалы, подлежащие последующему представлению;

42.4. последствия невыполнения установленных условий.

43. В признании эквивалентности отказывается, если:

43.1. документ либо комплект документов не относится к соответствующей национальной критической инфраструктуре;

43.2. отсутствуют существенные элементы;

43.3. документ устарел, является неполным либо неприменимым;

43.4. документ не согласуется с оценкой рисков;

43.5. документ не позволяет проверить меры, обязанности и механизмы их реализации;

43.6. документ не может быть рассмотрен с соблюдением применимого режима доступа.

44. Отказ в признании эквивалентности не освобождает управляющего от обязанности разработать и направить на согласование План безопасности в срок, установленный Методологическими нормами согласно приложению
№ 2. Инициирование и проведение процедуры признания эквивалентности не приостанавливают и не продлевают срок, установленный для разработки и направления Плана безопасности на согласование.

X. АКТ О ПРИЗНАНИИ ЭКВИВАЛЕНТНОСТИ

ИЛИ ОБ ОТКАЗЕ В ЕЕ ПРИЗНАНИИ

45. Результат рассмотрения оформляется актом о признании эквивалентности или об отказе в ее признании, издаваемым ответственным органом публичной власти.

46. Акт о признании эквивалентности или об отказе в ее признании должен содержать по меньшей мере:

46.1. идентификационные данные управляющего;

46.2. наименование национальной критической инфраструктуры;

46.3. сектор или подсектор, относящийся к компетенции ответственного органа публичной власти;

46.4. рассмотренные документы;

46.5. основание обращения;

46.6. таблицу соответствия или ее краткое изложение;

46.7. заключение по результатам рассмотрения;

46.8. форму признания эквивалентности, в соответствующих случаях: в полном объеме, частичное или условное;

46.9. элементы, признанные эквивалентными;

46.10. элементы, требующие дополнения, обновления или согласования;

46.11. срок устранения недостатков, в соответствующих случаях;

46.12. обязанности управляющего по применению, тестированию, пересмотру и обновлению документов, признанных эквивалентными;

46.13. дату издания;

46.14. подпись уполномоченного лица.

47. В случае признания эквивалентности в полном объеме документ или комплект документов, признанный эквивалентным, имеет те же функциональные последствия, что и План безопасности.

48. В случае частичного или условного признания эквивалентности документы, признанные эквивалентными, дополняются разделами, приложениями или документами, необходимыми для полного охвата минимальных требований к Плану безопасности.

49. Ответственный орган публичной власти ведет учет обращений о признании эквивалентности, рассмотренных документов и изданных актов.

XI. ПОСЛЕДСТВИЯ ПРИЗНАНИЯ ЭКВИВАЛЕНТНОСТИ

50. Документ или комплект документов, признанный эквивалентным, имеет функциональные последствия Плана безопасности в пределах и на условиях, установленных актом о признании эквивалентности.

51. В случае признания эквивалентности управляющий обязан обеспечить:

51.1. сохранение действительности документа или документов, признанных эквивалентными;

51.2. фактическое применение предусмотренных мер;

51.3. их обновление и пересмотр в соответствии с условиями, предусмотренными законом и настоящим постановлением;

51.4. сохранение соответствия документов, признанных эквивалентными, фактическому состоянию национальной критической инфраструктуры;

51.5. защиту информации, содержащейся в документах, признанных эквивалентными.

52. Признание эквивалентности не исключает обязанности управляющего дополнять или обновлять соответствующие документы при наступлении существенных изменений.

XII. ПЕРЕСМОТР ДОКУМЕНТОВ, ПРИЗНАННЫХ ЭКВИВАЛЕНТНЫМИ

53. К документам, признанным эквивалентными, применяются те же требования в отношении периодического и внеочередного пересмотра, что и к Плану безопасности.

54. Управляющий уведомляет ответственный орган публичной власти о любом изменении документа или комплекта документов, признанных эквивалентными, в срок не более 10 рабочих дней с даты утверждения изменения или вступления его в силу. Существенные изменения отражаются в обновленной документации по признанию эквивалентности, которая направляется ответственному органу публичной власти одновременно с уведомлением.

55. Если в результате пересмотра или внесенных изменений документы, признанные эквивалентными, более не охватывают минимальные требования, применимые к Плану безопасности, признание эквивалентности подлежит пересмотру.

56. В случае, предусмотренном пунктом 55, ответственный орган публичной власти вправе, в зависимости от обстоятельств:

56.1. сохранить признание эквивалентности, если несоответствия являются незначительными и могут быть устранены;

56.2. предоставить время для устранения недостатков;

56.3. прекратить действие признания эквивалентности и обязать управляющего разработать либо дополнить План безопасности в качестве отдельного документа.

57. Признание эквивалентности утрачивает силу, если:

57.1. документ, признанный эквивалентным, отменен, заменен или прекращает применяться;

57.2. национальная критическая инфраструктура претерпевает существенные изменения;

57.3. оценка рисков указывает на новые риски или существенные изменения профиля риска;

57.4. документ более не охватывает минимальные требования к Плану безопасности;

57.5. документ более не применяется или не может быть проверен;

57.6. по результатам тестирования, контроля, аудита или вследствие инцидентов выявлены существенные недостатки;

57.7. в национальную нормативную базу в области управления кризисами, устойчивости или защиты критических инфраструктур вносятся существенные изменения, требующие пересмотра документа либо комплекта документов, признанных эквивалентными.

XIII. СВОДНАЯ ЗАПИСКА О ПРИЗНАНИИ ЭКВИВАЛЕНТНОСТИ

58. К обращению о признании эквивалентности прилагается сводная записка, составленная управляющим.

59. Сводная записка о признании эквивалентности должна содержать по меньшей мере:

59.1. идентификационные данные управляющего;

59.2. наименование национальной критической инфраструктуры;

59.3. перечень документов, предлагаемых для признания эквивалентными;

59.4. обоснование обращения;

59.5. краткое описание соответствующего содержания документов;

59.6. сведения об их утверждении и действительности;

59.7. порядок соотнесения документов с типовой структурой Плана безопасности;

59.8. подтверждение принятия ответственности руководством управляющего.

XIV. ЗАЩИТА ИНФОРМАЦИИ

60. Обращение с документами, предлагаемыми для признания эквивалентными, таблицей соответствия, сводной запиской, актом о признании эквивалентности или об отказе в ее признании и сопутствующими документами осуществляется с соблюдением правового режима, применимого к информации, отнесенной к государственной тайне, персональным данным, чувствительной информации о национальных критических инфраструктурах и другим категориям информации, охраняемой законом.

61. Рассмотрение и признание эквивалентными документов, относящихся к национальным критическим инфраструктурам в области обороны, общественного порядка и государственной безопасности, осуществляются с соблюдением правового режима, применимого к информации, отнесенной к государственной тайне, чувствительной информации о национальных критических инфраструктурах и другим категориям информации, охраняемой законом. Передача, ознакомление, проверка, хранение и возврат документов, предлагаемых для признания эквивалентными, осуществляются с использованием соответствующих средств и уполномоченными лицами в соответствии с применимой нормативной базой.

62. Доступ к документам, предлагаемым для признания эквивалентными, предоставляется только лицам, непосредственно выполняющим соответствующие обязанности и обосновавшим необходимость работы с такой информацией.

63. Передача документов, предлагаемых для признания эквивалентными, осуществляется с использованием средств, обеспечивающих надлежащую защиту информации в соответствии с применимым правовым режимом.

64. Информация об уязвимостях, сценариях рисков, мерах безопасности, возможностях реагирования, уязвимых элементах и критических взаимозависимостях защищается соразмерно уровню риска, возникающего в результате ее разглашения.

XV. ОБЩИЕ ПРАВИЛА ПРИМЕНЕНИЯ И МЕТОДОЛОГИЧЕСКОГО СОГЛАСОВАНИЯ

65. Процедура признания эквивалентности применяется с соблюдением принципа пропорциональности, без снижения уровня защиты, безопасности и непрерывности, необходимого для национальной критической инфраструктуры.

66. Во всех случаях документ либо комплект документов может быть признан эквивалентным только при условии, что он позволяет:

66.1. четко идентифицировать соответствующие риски;

66.2. организовать меры безопасности;

66.3. обеспечивать непрерывность основной услуги;

66.4. координировать реагирование и восстановление;

66.5. проводить проверку, обновление и периодический пересмотр.

67. Признание существующих документов эквивалентными Плану безопасности не исключает обязанности управляющего соблюдать правовые, секторальные, технические и процедурные требования, применимые к национальной критической инфраструктуре.

68. Ответственные органы публичной власти могут разрабатывать типовые формы таблиц соответствия, секторальные инструкции или рекомендации по применению настоящих Методологических норм с информированием Национального центра по координации защиты критических инфраструктур.

69. Национальный центр по координации защиты критических инфраструктур издает методологические рекомендации по единообразному применению процедуры признания эквивалентности.

70. Во всех случаях документы, признанные эквивалентными, должны позволять достичь того же уровня защиты, непрерывности, реагирования, восстановления и устойчивости, что и План безопасности, разработанный в соответствии с типовой структурой, предусмотренной приложением № 3.

71. Управляющий обеспечивает прослеживаемость соответствия между минимальными требованиями к Плану безопасности и существующими документами, предлагаемыми для признания эквивалентными, в том числе посредством составления и ведения внутреннего реестра или таблицы соответствия, в которых указываются документы, разделы, процедуры либо приложения, посредством которых каждое требование охватывается полностью или частично.

Приложение № 5

к Постановлению Правительства

№ 483/2026

МЕТОДОЛОГИЧЕСКИЕ НОРМЫ

пересмотра и обновления Плана безопасности управляющего

Национальной критической инфраструктурой

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Методологические нормы устанавливают порядок пересмотра и обновления Плана безопасности управляющего национальной критической инфраструктурой (в дальнейшем – *План безопасности*).

2. Пересмотр и обновление Плана безопасности осуществляются в целях поддержания его актуальности, применимости, согласованности и эффективности с учетом динамики рисков, изменений национальной критической инфраструктуры, изменений операционного, технологического, организационного, законодательного или отраслевого характера, а также выводов, сделанных по результатам инцидентов, тестирований, учений, аудитов или проверок.

3. Для целей настоящих Методологических норм:

3.1. обновление – точечное изменение отдельных данных, глав, приложений, процедур, обязанностей или мер Плана безопасности без изменения его общей структуры;

3.2. пересмотр – процесс систематического повторного рассмотрения Плана безопасности в целях проверки его актуальности, применимости, соответствия и согласованности с оценкой рисков и фактическим состоянием национальной критической инфраструктуры;

3.3. периодический пересмотр – пересмотр, осуществляемый через регулярные промежутки времени в сроки, установленные настоящими Методологическими нормами или применимыми отраслевыми нормативными положениями;

3.4. внеочередной пересмотр – пересмотр, инициируемый в связи с возникновением инцидента, появлением новых рисков, уязвимостей или существенных изменений либо по запросу ответственного органа публичной власти.

4. Пересмотр и обновление Плана безопасности осуществляются управляющим национальной критической инфраструктурой (в дальнейшем – *управляющий*) во взаимодействии с соответствующими внутренними структурами и, при необходимости, с ответственным органом публичной власти соответствующего сектора или подсектора.

5. Офицер связи по безопасности национальной критической инфраструктуры

координирует на оперативном уровне процесс пересмотра и обновления Плана безопасности, при этом ответственность руководства управляющего сохраняется.

6. Пересмотр и обновление Плана безопасности осуществляются с соблюдением требований к защите информации, отнесенной к государственной тайне, персональных данных, чувствительной информации о национальных критических инфраструктурах и иных категорий информации, охраняемой законом.

7. Пересмотр и обновление Плана безопасности осуществляются с соблюдением правового режима, применимого к информации, отнесенной к государственной тайне, чувствительной информации о национальных критических инфраструктурах и иным категориям информации, охраняемой законом. Передача, рассмотрение, утверждение и хранение пересмотренных или обновленных версий осуществляются с использованием соответствующих средств и уполномоченными лицами.

II. ПЕРИОДИЧЕСКИЙ ПЕРЕСМОТР

8. План безопасности подлежит периодическому пересмотру не реже одного раза в два года, если законом, актом о назначении национальной критической инфраструктуры или отраслевыми нормативными положениями не установлен более короткий срок. Периодический пересмотр осуществляется во взаимосвязи с периодическим тестированием Плана безопасности, предусмотренным приложением № 2, а результаты тестирований, учений и моделирований учитываются при его пересмотре и обновлении.

9. В рамках периодического пересмотра проверяются:

9.1. данные об управляющем и национальной критической инфраструктуре;

9.2. описание предоставляемой основной услуги;

9.3. оценка рисков и установленных уровней риска;

9.4. значимость выявленных рисков;

9.5. критические функции, критические активы и основные процессы;

9.6. зависимость и взаимозависимости;

9.7. актуальность и эффективность существующих мер безопасности, предотвращения, непрерывности, реагирования и восстановления;

9.8. наличие и актуальность реестра рисков национальной критической инфраструктуры;

9.9. степень реализации мер, предусмотренных Планом безопасности;

9.10. работоспособность механизмов уведомления, коммуникации и координации;

9.11. актуальность перечней контактных данных, обязанностей и связанных с ними процедур;

9.12. результаты проведенных мероприятий по подготовке, тестирований и учений;

9.13. необходимость дополнения, изменения или исключения отдельных глав, разделов или приложений.

10. Результаты периодического пересмотра оформляются управляющим в виде записки об обновлении/пересмотре.

11. Если по результатам периодического пересмотра необходимость внесения изменений не установлена, это указывается в записке об обновлении/пересмотре с приведением соответствующего обоснования.

III. ВНЕОЧЕРЕДНОЙ ПЕРЕСМОТР

12. Внеочередной пересмотр инициируется при возникновении событий, изменений или выявлении обстоятельств, способных повлиять на актуальность, применимость, соответствие требованиям или эффективность Плана безопасности.

13. Внеочередной пересмотр инициируется, в частности, в следующих случаях:

13.1. возникновения крупного инцидента, который затрагивает или может затронуть национальную критическую инфраструктуру либо предоставляемую основную услугу;

13.2. возникновения значительного нарушения функционирования национальной критической инфраструктуры;

13.3. выявления новых рисков, угроз, уязвимостей или сценариев риска;

13.4. изменения уровня существующих рисков;

13.5. изменения оценки рисков или реестра рисков;

13.6. структурных, технологических, функциональных или организационных изменений национальной критической инфраструктуры;

13.7. изменения критических функций, критических активов или основных процессов;

13.8. изменения соответствующих зависимостей или взаимозависимостей;

13.9. смены критических поставщиков, поставщиков услуг, цепочек поставок или механизмов технической поддержки;

13.10. получения значимых результатов аудитов, проверок, тестирований, учений или моделирований;

13.11. выявления недостатков при применении мер безопасности, обеспечения непрерывности, реагирования или восстановления;

13.12. изменения применимой нормативной базы или отраслевых требований;

13.13. изменения акта о назначении национальной критической инфраструктуры;

13.14. изменения режима собственности, управления, эксплуатации или контроля в отношении национальной критической инфраструктуры;

13.15. поступления запроса ответственного органа публичной власти;

13.16. поступления запроса Национального центра по координации защиты критических инфраструктур (в дальнейшем – *НЦКЗКИ*) в соответствии с законом;

13.17. объявления кризисного состояния или изменения уровня оповещения на национальном уровне, если это затрагивает или может затронуть функционирование национальной критической инфраструктуры либо непрерывность предоставляемой основной услуги;

13.18. установления того, что документы, признанные эквивалентными, более не охватывают минимальные требования к Плану безопасности;

13.19. возникновения любой иной ситуации, способной повлиять на защиту, безопасность, непрерывность, реагирование, восстановление или устойчивость национальной критической инфраструктуры.

14. Внеочередной пересмотр инициируется незамедлительно после установления обстоятельства, послужившего основанием для его проведения.

15. В случае возникновения крупного инцидента или выявления существенной уязвимости управляющий может применять временные или компенсирующие меры до завершения пересмотра Плана безопасности.

IV. ИНИЦИИРОВАНИЕ ПРОЦЕССА ПЕРЕСМОТРА ИЛИ ОБНОВЛЕНИЯ

16. Процесс пересмотра или обновления инициируется по решению руководства управляющего национальной критической инфраструктурой либо по предложению офицера связи, структуры, ответственной за безопасность, непрерывность деятельности или управление рисками, либо иной соответствующей внутренней структуры.

17. Пересмотр или обновление могут быть инициированы также по запросу ответственного органа публичной власти в пределах его установленных законом полномочий.

18. Решением об инициировании пересмотра или обновления, в зависимости от

обстоятельств, определяются:

18.1. основание для пересмотра или обновления;

18.2. предмет пересмотра или обновления;

18.3. главы, разделы, приложения или процедуры, подлежащие пересмотру или обновлению;

18.4. задействованные структуры и лица;

18.5. координатор процесса;

18.6. срок проведения;

18.7. порядок документирования результатов.

19. В зависимости от сложности изменений управляющий может создать внутреннюю рабочую группу или внутреннюю комиссию для пересмотра или обновления Плана безопасности.

V. ПРОВЕДЕНИЕ ПЕРЕСМОТРА

20. Пересмотр Плана безопасности включает рассмотрение по меньшей мере следующих элементов:

20.1. оценки рисков и реестра рисков;

20.2. соответствующих сценариев риска;

20.3. критических функций, критических активов и основных процессов;

20.4. зависимостей и взаимозависимостей;

20.5. существующих мер безопасности;

20.6. дополнительных мер и стадии их реализации;

20.7. мер по обеспечению непрерывности деятельности;

20.8. мер реагирования, уведомления и восстановления;

20.9. внутренних обязанностей и механизмов координации;

20.10. механизмов коммуникации, отчетности и обмена информацией;

20.11. программы подготовки, тестирования и учений;

20.12. приложений, реестров, перечней контактных данных и связанных с ними процедур;

20.13. режима документа и защиты информации.

21. В ходе пересмотра проверяется, насколько План безопасности:

21.1. соответствует фактическому состоянию национальной критической инфраструктуры;

21.2. согласован с актуальной оценкой рисков;

21.3. предусматривает меры, соразмерные уровню рисков;

21.4. четко определяет обязанности;

21.5. предусматривает сроки, ресурсы и показатели выполнения;

21.6. обеспечивает возможность скоординированного реагирования в случае инцидента;

21.7. обеспечивает непрерывность основной услуги;

21.8. обеспечивает возможность восстановления затронутых критических функций;

21.9. доведен до сведения ответственных структур и может применяться ими;

21.10. нуждается в изменении, дополнении или обновлении.

22. Если по результатам пересмотра установлено изменение профиля риска, управляющий обновляет оценку рисков в соответствии с Методологическими нормами оценки рисков для национальных критических инфраструктур, предусмотренными приложением № 1.

23. Если по результатам пересмотра установлена необходимость изменения содержания Плана безопасности, управляющий обновляет соответствующие главы, разделы, приложения или процедуры.

VI. КЛАССИФИКАЦИЯ ИЗМЕНЕНИЙ

24. Изменения, вносимые в План безопасности, в зависимости от их характера подразделяются на:

24.1. незначительные изменения;

24.2. значительные изменения;

24.3. существенные изменения.

25. Незначительными являются изменения, которые не затрагивают основное содержание Плана безопасности, профиль риска, основные меры, основные обязанности или механизмы уведомления и координации.

26. К незначительным изменениям могут относиться:

26.1. обновление контактных данных;

26.2. обновление наименований отдельных внутренних структур без изменения их полномочий;

26.3. исправление технических ошибок;

26.4. обновление оперативных перечней без изменения основных механизмов;

26.5. внесение редакционных изменений или изменений оформления, не затрагивающих основное содержание Плана безопасности.

27. Значительными являются изменения, которые затрагивают отдельные главы, разделы, приложения, меры, обязанности или процедуры Плана безопасности, но не требуют его полного пересмотра.

28. К значительным изменениям могут относиться:

28.1. введение или изменение отдельных мер безопасности, обеспечения непрерывности, реагирования или восстановления;

28.2. изменение основных оперативных обязанностей;

28.3. изменение отдельных процедур уведомления, коммуникации или эскалации;

28.4. изменение отдельных соответствующих зависимостей или взаимозависимостей;

28.5. изменение отдельных важных технических приложений;

28.6. изменение отдельных сроков, ресурсов или показателей реализации.

29. Существенными являются изменения, которые затрагивают общую структуру Плана безопасности, профиль риска, критические функции, критические активы, основную услугу, основные меры безопасности либо способность обеспечивать непрерывность и восстановление.

30. Существенные изменения требуют полного пересмотра Плана безопасности или, в зависимости от обстоятельств, разработки его новой версии.

VII. РЕЗУЛЬТАТЫ ПЕРЕСМОТРА И УТВЕРЖДЕНИЕ ИЗМЕНЕНИЙ

31. По результатам пересмотра управляющий может принять, в зависимости от обстоятельств, одно из следующих решений:

31.1. оставить План безопасности без изменений;

31.2. частично обновить План безопасности;

31.3. провести полный пересмотр Плана безопасности;

31.4. разработать новую версию Плана безопасности;

31.5. обновить оценку рисков;

31.6. обновить документы, признанные эквивалентными;

31.7. направить План безопасности на повторное согласование в случаях, предусмотренных настоящими Методологическими нормами.

32. Результаты процесса обновления или пересмотра оформляются управляющим в виде записки об обновлении/пересмотре.

33. Записка об обновлении/пересмотре содержит по меньшей мере:

33.1. основание для обновления или пересмотра;

33.2. описание обстоятельств, обусловивших внесение изменений;

33.3. элементы Плана безопасности, затронутые изменениями;

33.4. влияние на оценку рисков;

33.5. предлагаемые изменения;

33.6. заключение;

33.7. ответственных лиц;

33.8. сроки реализации;

33.9. необходимость повторного согласования, в зависимости от обстоятельств;

33.10. выводы, сделанные по результатам анализа опыта управления инцидентами, кризисными ситуациями и проведения межведомственных учений, в зависимости от обстоятельств;

33.11. меры, определенные для учета и практической реализации сделанных выводов, ответственных лиц и соответствующие сроки.

34. Незначительные изменения утверждаются в соответствии с внутренними процедурами управляющего и отражаются в учете изменений Плана безопасности.

35. Значительные и существенные изменения утверждаются руководителем управляющего национальной критической инфраструктурой или компетентным лицом, назначенным в соответствии с применимыми внутренними актами.

36. В обновленной версии Плана безопасности прямо указываются дата вступления в силу, номер версии и изменения, внесенные по сравнению с предыдущей версией.

VIII. ПОВТОРНОЕ СОГЛАСОВАНИЕ ПЛАНА БЕЗОПАСНОСТИ

37. Обновленный План безопасности направляется на повторное согласование ответственному органу публичной власти, если внесенные изменения затрагивают:

37.1. оценку рисков;

37.2. приоритетные риски;

37.3. критические функции, критические активы или основные процессы;

37.4. предоставляемую основную услугу;

37.5. основные меры безопасности, обеспечения непрерывности, реагирования или восстановления;

37.6. основные обязанности;

37.7. механизмы уведомления, коммуникации, отчетности или координации;

37.8. соответствующие зависимости или взаимозависимости;

37.9. документы, признанные эквивалентными;

37.10. режим документа или защиту информации, если изменение может повлиять на доступ к информации или ее обращение;

37.11. механизмы сотрудничества и координации с компетентными органами в рамках Национальной системы управления кризисами.

38. Незначительные изменения, не затрагивающие элементы, предусмотренные пунктом 37, не требуют повторного согласования при условии их отражения в учете изменений Плана безопасности.

39. Ответственный орган публичной власти рассматривает обновленную редакцию Плана безопасности в соответствии с процедурой согласования, предусмотренной приложением № 2.

40. Если ответственный орган публичной власти устанавливает, что внесенные изменения не требуют повторного согласования, он может принять обновление к сведению и, при необходимости, потребовать хранения подтверждающих документов в учете управляющего.

IX. ПОСЛЕДСТВИЯ ПЕРЕСМОТРА ДЛЯ ДОКУМЕНТОВ,

ПРИЗНАННЫХ ЭКВИВАЛЕНТНЫМИ

41. Если План безопасности полностью или частично состоит из документов, признанных эквивалентными, пересмотр Плана безопасности включает также проверку указанных документов.

42. Документы, признанные эквивалентными, подлежат пересмотру при возникновении любых изменений, влияющих на их актуальность, применимость или соответствие минимальным требованиям, предусмотренным типовой структурой Плана безопасности согласно приложению № 3.

43. Если документы, признанные эквивалентными, более не охватывают в полном объеме или в достаточной степени требования к Плану безопасности, управляющий:

43.1. обновляет соответствующие документы;

43.2. дополняет документы дополнительными разделами или приложениями;

43.3. при необходимости обращается за их повторным признанием эквивалентными;

43.4. разрабатывает План безопасности в виде отдельного документа, если признание эквивалентности более не может сохраняться.

44. Управляющий национальной критической инфраструктурой уведомляет ответственный орган публичной власти о прекращении действия, приостановлении действия или существенном изменении документа либо комплекта документов, признанных эквивалентными, в срок не более 10 рабочих дней с даты наступления соответствующего обстоятельства.

X. УЧЕТ И ПРОСЛЕЖИВАЕМОСТЬ ПЕРЕСМОТРА

45. Управляющий национальной критической инфраструктурой обеспечивает учет и прослеживаемость всех случаев пересмотра и обновления Плана безопасности.

46. Учет пересмотров и обновлений включает по меньшей мере:

46.1. дату инициирования пересмотра или обновления;

46.2. основание для пересмотра или обновления;

46.3. главы, разделы, приложения или процедуры, затронутые изменениями;

46.4. описание внесенных изменений;

46.5. ответственных лиц или структуры;

46.6. дату утверждения изменений;

46.7. необходимость повторного согласования, в зависимости от обстоятельств;

46.8. дату направления на повторное согласование, в зависимости от обстоятельств;

46.9. новую версию Плана безопасности;

46.10. подтверждающие документы.

47. Управляющий обеспечивает:

47.1. хранение записок об обновлении/пересмотре;

47.2. хранение предыдущих версий Плана безопасности;

47.3. учет внесенных изменений;

47.4. хранение подтверждающих документов, послуживших основанием для пересмотра;

47.5. изъятие из обращения или архивирование устаревших версий;

47.6. информирование соответствующих внутренних структур о действующей версии.

48. Предыдущие версии Плана безопасности хранятся в соответствии с правовым режимом, применимым к документу, и внутренними правилами архивирования.

XI. ЗАЩИТА ИНФОРМАЦИИ В ПРОЦЕССЕ ПЕРЕСМОТРА И ОБНОВЛЕНИЯ

49. Документы, составленные в процессе пересмотра и обновления, включая записки об обновлении/пересмотре, предыдущие версии, подтверждающие документы и затронутые изменениями приложения, обрабатываются с соблюдением правового режима, применимого к информации, отнесенной к государственной тайне, персональным данным, чувствительной информации о национальных критических инфраструктурах и иным категориям информации, охраняемой законом.

50. Доступ к документам, относящимся к процессу пересмотра и обновления, предоставляется только лицам, на которых возложены соответствующие обязанности и для которых работа с такой информацией обусловлена служебной необходимостью.

51. Передача документов, относящихся к пересмотру и обновлению, ответственному органу публичной власти или иным уполномоченным субъектам осуществляется средствами, обеспечивающими надлежащую защиту информации в соответствии с применимым к ней правовым режимом.

52. Информация об уязвимостях, сценариях риска, мерах безопасности, возможностях реагирования, уязвимых местах, критических взаимозависимостях и недостатках, выявленных в процессе пересмотра, защищается соразмерно уровню риска, возникающего в случае ее разглашения.

XII. ОБЩИЕ ПРАВИЛА ПРИМЕНЕНИЯ И МЕТОДОЛОГИЧЕСКОГО СОГЛАСОВАНИЯ

53. Пересмотр и обновление Плана безопасности не освобождают управляющего от обязанности применять действующие меры безопасности, обеспечения непрерывности, реагирования и восстановления.

54. В период пересмотра управляющий обеспечивает непрерывное применение существующих мер, а при необходимости – временных или компенсирующих мер в отношении выявленных рисков.

55. Пересмотр и обновление Плана безопасности осуществляются без снижения уровня защиты, непрерывности и устойчивости национальной критической инфраструктуры и должны, при необходимости, способствовать укреплению национальной устойчивости и обеспечению непрерывности жизненно важных функций государства в соответствии с нормативной базой в области управления кризисами.

56. Ответственные органы публичной власти могут разрабатывать отраслевые инструкции, рекомендации, образцы реестров или вспомогательные инструменты для применения настоящих Методологических норм с информированием НЦКЗКИ.

57. НЦКЗКИ предоставляет ответственным органам публичной власти и управляющим национальными критическими инфраструктурами образцы записок об обновлении/пересмотре, реестров учета изменений и иные вспомогательные методологические инструменты.

58. Положения настоящего приложения применяются соответствующим образом также к документам, признанным эквивалентными Плану безопасности.

Приложение № 6

к Постановлению Правительства

№ 483/2026

МЕТОДОЛОГИЧЕСКИЕ НОРМЫ,

определяющие порядок назначения, функциональный статус

и обязанности офицера связи по безопасности национальной

критической инфраструктуры

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Методологические нормы определяют порядок назначения, функциональный статус, минимальные требования и обязанности офицера связи по безопасности национальной критической инфраструктуры (в дальнейшем – *офицер связи*), назначаемого на уровне управляющего национальной критической инфраструктурой (в дальнейшем – *управляющий*), а также обязанности контактного пункта, назначаемого на уровне ответственного органа публичной власти.

2. Офицер связи обеспечивает оперативную координацию, коммуникацию и обмен соответствующей информацией по вопросам защиты, безопасности, непрерывности, реагирования, восстановления и устойчивости национальной критической инфраструктуры.

3. Назначение офицера связи не освобождает руководство управляющего национальной критической инфраструктурой от ответственности и не влечет передачи ему полномочий компетентных внутренних структур. Офицер связи обеспечивает координацию и функциональное взаимодействие между указанными субъектами, ответственным органом публичной власти и, при необходимости, Национальным центром по координации защиты критических инфраструктур (в дальнейшем – *НЦКЗКИ*).

4. Для целей настоящих Методологических норм под офицером связи понимается лицо, назначенное управляющим национальной критической инфраструктурой для выполнения обязанностей по координации, коммуникации и оказанию содействия в вопросах безопасности национальной критической инфраструктуры.

5. На уровне ответственного органа публичной власти назначается контактный пункт или ответственное лицо для взаимодействия с управляющими соответствующего сектора или подсектора и НЦКЗКИ.

II. НАЗНАЧЕНИЕ ОФИЦЕРА СВЯЗИ НА УРОВНЕ УПРАВЛЯЮЩЕГО

6. Управляющий назначает офицера связи.

7. Если один управляющий управляет или эксплуатирует несколько объектов национальной критической инфраструктуры, он может назначить:

7.1. офицера связи для каждого объекта национальной критической инфраструктуры;

7.2. одного офицера связи для нескольких объектов национальной критической инфраструктуры при условии обеспечения возможности эффективного выполнения им своих обязанностей;

7.3. координатора на центральном уровне и ответственных лиц на уровне каждого объекта национальной критической инфраструктуры.

8. В целях обеспечения непрерывности коммуникации управляющий назначает лицо, замещающее офицера связи.

9. Офицер связи и замещающее его лицо назначаются внутренним актом управляющего национальной критической инфраструктурой.

10. Внутренний акт о назначении должен содержать как минимум:

10.1. фамилию и имя назначенного лица;

10.2. занимаемую им должность в структуре управляющего;

10.3. национальную критическую инфраструктуру, для которой оно назначено;

10.4. основные обязанности;

10.5. служебные контактные данные;

10.6. фамилию и имя лица, назначенного для замещения офицера связи;

10.7. дату, с которой назначение вступает в силу;

10.8. обязанности по соблюдению конфиденциальности и защите информации.

11. Управляющий информирует ответственный орган публичной власти о назначении или замене офицера связи и замещающего его лица, а также об изменении их контактных данных в течение 7 рабочих дней со дня соответствующего изменения.

12. Ответственный орган публичной власти может представлять Национальному центру по координации защиты критических инфраструктур обобщенную информацию об офицерах связи, назначенных на уровне управляющих соответствующего сектора или подсектора.

III. ФУНКЦИОНАЛЬНЫЙ СТАТУС

И УСЛОВИЯ ВЫПОЛНЕНИЯ ОБЯЗАННОСТЕЙ

13. Офицер связи выполняет обязанности, установленные настоящим приложением, внутренним актом о назначении и внутренними документами управляющего национальной критической инфраструктурой.

14. Офицеру связи должен быть предоставлен доступ к информации, документам, структурам и процессам, необходимым для выполнения его обязанностей, с соблюдением правового режима, применимого к защищаемой информации.

15. Управляющий обеспечивает организационные условия, необходимые для выполнения обязанностей офицером связи, включая:

15.1. доступ к соответствующей информации;

15.2. участие во внутренних процессах, связанных с оценкой рисков и Планом безопасности;

15.3. участие в соответствующих заседаниях, учениях, тестировании, обучении и консультациях;

15.4. взаимодействие с ответственным органом публичной власти;

15.5. взаимодействие с внутренними структурами, ответственными за

безопасность, непрерывность, реагирование и восстановление.

16. Офицер связи может совмещать обязанности, предусмотренные настоящим приложением, с иными служебными обязанностями при условии, что такое совмещение не препятствует надлежащему выполнению обязанностей в области безопасности национальной критической инфраструктуры.

17. Офицер связи выполняет свои обязанности в пределах полномочий, предоставленных ему управляющим, и не наделяется правом оперативного руководства или принятия решений за пределами полномочий, установленных внутренним актом о назначении. Оперативные решения принимаются, а обязательные меры устанавливаются руководством управляющего либо компетентными внутренними структурами в соответствии с их полномочиями.

IV. ОБЩИЕ ОБЯЗАННОСТИ ОФИЦЕРА СВЯЗИ

18. Офицер связи выполняет следующие общие обязанности:

18.1. обеспечивает оперативное взаимодействие между управляющим и ответственным органом публичной власти;

18.2. обеспечивает, при необходимости, взаимодействие с Национальным центром по координации защиты критических инфраструктур через ответственный орган публичной власти либо в соответствии с установленными механизмами;

18.3. координирует на оперативном уровне внутреннюю деятельность, связанную с защитой, безопасностью, непрерывностью и устойчивостью национальной критической инфраструктуры;

18.4. участвует в сборе, обновлении и систематизации соответствующей информации о национальной критической инфраструктуре;

18.5. оказывает содействие руководству управляющего в мониторинге выполнения обязательств, связанных с национальной критической инфраструктурой;

18.6. следит за обеспечением взаимосвязи между оценкой рисков, Планом безопасности и реализуемыми мерами;

18.7. содействует обмену информацией между ответственными внутренними структурами;

18.8. участвует в подготовке документов, информации и отчетов, запрашиваемых ответственным органом публичной власти, в пределах установленных законом полномочий;

18.9. информирует руководство управляющего о существенных проблемах, выявленных в процессе реализации мер безопасности;

18.10. содействует ведению учета и обновлению данных, относящихся к национальной критической инфраструктуре.

V. ОБЯЗАННОСТИ В ОБЛАСТИ ОЦЕНКИ РИСКОВ

И ПЛАНА БЕЗОПАСНОСТИ

19. В области оценки рисков офицер связи:

19.1. участвует в организации процесса оценки рисков;

19.2. содействует сбору информации, необходимой для оценки рисков;

19.3. участвует в определении критических функций, критических активов, основных процессов, зависимостей и взаимозависимостей;

19.4. содействует выявлению рисков, угроз, уязвимостей и соответствующих сценариев;

19.5. участвует в обновлении реестра рисков, карточек рисков и связанных с ними документов;

19.6. информирует руководство управляющего об изменениях, которые могут повлиять на профиль риска национальной критической инфраструктуры.

20. В области Плана безопасности офицер связи:

20.1. координирует на оперативном уровне разработку, обновление и пересмотр Плана безопасности;

20.2. содействует согласованию Плана безопасности с оценкой рисков;

20.3. следит за включением в План безопасности мер в отношении выявленных рисков;

20.4. участвует в дополнении, обновлении и систематизации приложений к Плану безопасности;

20.5. содействует проведению консультаций с соответствующими внутренними структурами;

20.6. следит за ведением учета версий Плана безопасности;

20.7. участвует в подготовке документов, необходимых для согласования, повторного согласования или признания эквивалентности, в зависимости от случая;

20.8. осуществляет на оперативном уровне мониторинг хода реализации мер, предусмотренных Планом безопасности;

20.9. информирует руководство управляющего о задержках, несоответствиях или трудностях при реализации мер.

21. Офицер связи участвует в документальном оформлении обновления и пересмотра Плана безопасности, в том числе в подготовке либо координации

подготовки записки об обновлении/пересмотре, в зависимости от случая.

VI. ОБЯЗАННОСТИ В ОБЛАСТИ СОТРУДНИЧЕСТВА, ОТЧЕТНОСТИ И МОНИТОРИНГА

22. В области сотрудничества, отчетности и мониторинга офицер связи:

22.1. поддерживает взаимодействие с ответственным органом публичной власти;

22.2. в пределах предоставленных полномочий передает информацию, запрашиваемую ответственным органом публичной власти;

22.3. содействует подготовке ответов на запросы ответственного органа публичной власти;

22.4. в пределах полномочий управляющего и в соответствии с процедурами, предусмотренными применимой нормативной базой, участвует в представлении информации об инцидентах, нарушениях функционирования, уязвимостях или существенных изменениях без создания параллельного механизма уведомления;

22.5. содействует взаимодействию с поставщиками, исполнителями, партнерами и другими соответствующими субъектами в пределах предоставленных полномочий;

22.6. содействует мониторингу мер безопасности, непрерывности, реагирования и восстановления;

22.7. информирует руководство управляющего о запросах, рекомендациях или замечаниях, поступивших от ответственного органа публичной власти;

22.8. участвует в подготовке обобщенной информации о ходе реализации Плана безопасности;

22.9. при необходимости следит за устранением недостатков, выявленных по результатам проверок, аудитов, учений или инцидентов.

23. Офицер связи передает чувствительную, конфиденциальную или отнесенную к государственной тайне информацию исключительно в соответствии с применимым законодательством и в пределах полномочий, предоставленных руководством управляющего.

VII. ОБЯЗАННОСТИ В ОБЛАСТИ ОБУЧЕНИЯ, ТЕСТИРОВАНИЯ И УЧЕНИЙ

24. В области обучения, тестирования и учений офицер связи:

24.1. участвует в определении потребностей в обучении по вопросам безопасности национальной критической инфраструктуры;

24.2. содействует организации соответствующего внутреннего обучения;

24.3. участвует в планировании тестирования, моделирования и учений, связанных с Планом безопасности;

24.4. при необходимости участвует в учениях, проводимых на внутреннем, секторальном или межведомственном уровне;

24.5. содействует документированию результатов учений, тестирования и моделирования, а также участвует в определении извлеченных уроков и корректирующих мер;

24.6. следит за учетом соответствующих выводов в процессе пересмотра или обновления Плана безопасности;

24.7. содействует информированию соответствующего персонала об изменениях Плана безопасности.

VIII. МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ

К НАЗНАЧЕНИЮ ОФИЦЕРА СВЯЗИ

25. Лицо, назначаемое офицером связи, должно соответствовать как минимум следующим требованиям:

25.1. состоять в трудовых отношениях с управляющим национальной критической инфраструктурой либо выполнять обязанности в его структуре на основании соответствующих правоотношений;

25.2. знать специфику национальной критической инфраструктуры и предоставляемой основной услуги;

25.3. иметь доступ к структурам, процессам и информации, необходимым для выполнения своих обязанностей;

25.4. обладать способностью координировать внутреннее и внешнее взаимодействие;

25.5. знать соответствующие внутренние процедуры в области безопасности, непрерывности, реагирования и восстановления;

25.6. соблюдать требования конфиденциальности и защиты информации;

25.7. не находиться в состоянии несовместимости, установленной применимой нормативной базой, в ситуации конфликта интересов либо в ситуации, когда обязанности, выполняемые им в структуре управляющего национальной критической инфраструктурой, могут повлиять на беспристрастность, независимость или надлежащее выполнение обязанностей офицера связи.

26. В зависимости от специфики национальной критической инфраструктуры управляющий может устанавливать дополнительные требования в отношении:

26.1. профессионального опыта;

26.2. области специализации;

26.3. знаний в области управления рисками;

26.4. знаний в области непрерывности деятельности;

26.5. знаний в области физической, информационной, кибернетической или операционной безопасности;

26.6. участия в специализированном обучении;

26.7. допуска к информации, отнесенной к государственной тайне, если этого требует характер выполняемых обязанностей.

27. Управляющий обеспечивает периодическое участие офицера связи в соответствующих программах обучения, повышения квалификации или учениях, в том числе в области управления рисками, управления кризисными ситуациями, межведомственного сотрудничества и защиты национальных критических инфраструктур, в целях поддержания и развития компетенций, необходимых для выполнения его обязанностей.

28. Доступ офицера связи к информации, отнесенной к государственной тайне, или иной защищаемой информации предоставляется исключительно в соответствии с применимым законодательством.

IX. ОБЯЗАННОСТИ ПО СОБЛЮДЕНИЮ ПРАВИЛ ПОВЕДЕНИЯ И КОНФИДЕНЦИАЛЬНОСТИ

29. Офицер связи выполняет свои обязанности ответственно, беспристрастно и добросовестно, с соблюдением интересов обеспечения безопасности национальной критической инфраструктуры.

30. Офицер связи обязан:

30.1. соблюдать конфиденциальность информации, к которой он имеет доступ;

30.2. использовать информацию исключительно в целях выполнения своих обязанностей;

30.3. соблюдать правовой режим защищаемой информации;

30.4. не допускать несанкционированного разглашения информации об уязвимостях, рисках, сценариях, мерах безопасности, возможностях реагирования или уязвимых элементах;

30.5. информировать руководство управляющего о любых обстоятельствах, которые могут повлиять на выполнение им своих обязанностей;

30.6. соблюдать внутренние процедуры в отношении доступа к информации, ее хранения, передачи и архивирования.

31. Офицер связи не вправе использовать информацию, полученную при выполнении своих обязанностей, в иных целях, кроме предусмотренных настоящим приложением, внутренним актом о назначении и применимым законодательством.

X. ПРЕКРАЩЕНИЕ, ИЗМЕНЕНИЕ

И ОБНОВЛЕНИЕ НАЗНАЧЕНИЯ

32. Назначение офицера связи прекращается в следующих случаях:

32.1. прекращение трудовых или служебных отношений с управляющим;

32.2. изменение должности или обязанностей, если это препятствует выполнению функций офицера связи;

32.3. отмена назначения внутренним актом управляющего;

32.4. невозможность выполнения обязанностей в течение длительного периода;

32.5. установление несовместимости либо невозможности надлежащего выполнения обязанностей;

32.6. в иных случаях, предусмотренных внутренними актами управляющего или применимым законодательством.

33. В случае прекращения назначения управляющий назначает нового офицера связи и информирует об этом ответственный орган публичной власти в течение 5 рабочих дней.

34. В случае временного отсутствия офицера связи его обязанности выполняет назначенное замещающее лицо.

35. Управляющий обновляет сведения об офицере связи и замещающем его лице при любом изменении должности, контактных данных, обязанностей или возможности выполнения соответствующих функций.

XI. КОНТАКТНЫЙ ПУНКТ НА УРОВНЕ ОТВЕТСТВЕННОГО

ОРГАНА ПУБЛИЧНОЙ ВЛАСТИ

36. Ответственный орган публичной власти назначает на уровне специализированной или компетентной структуры контактный пункт по вопросам безопасности национальных критических инфраструктур соответствующего сектора или подсектора.

37. Контактный пункт, назначенный на уровне ответственного органа публичной власти, обеспечивает функциональное взаимодействие с управляющими национальной

критической инфраструктурой, их офицерами связи и Национальным центром по координации защиты критических инфраструктур.

38. Контактный пункт ответственного органа публичной власти выполняет следующие обязанности:

38.1. ведет учет офицеров связи, назначенных управляющими национальной критической инфраструктурой соответствующего сектора или подсектора;

38.2. обеспечивает взаимодействие управляющих с офицерами связи;

38.3. принимает информацию, уведомления, запросы и документы, направляемые управляющими, в пределах установленных законом полномочий;

38.4. содействует рассмотрению Планов безопасности, представленных для согласования или повторного согласования;

38.5. содействует рассмотрению запросов о признании существующих документов эквивалентными Плану безопасности;

38.6. участвует в мониторинге соблюдения управляющими законодательных и методологических требований;

38.7. обобщает информацию о ходе разработки, согласования, реализации, тестирования, пересмотра и обновления Планов безопасности;

38.8. обеспечивает представление НЦКЗКИ необходимой обобщенной информации без разглашения чувствительной информации, конфиденциальной или информации, отнесенной к государственной тайне, если применимым законодательством не предусмотрено иное;

38.9. участвует в заседаниях, консультациях, обучении, учениях и других соответствующих мероприятиях по вопросам защиты национальных критических инфраструктур;

38.10. содействует единообразному применению методологических требований в соответствующем секторе или подсекторе;

38.11. информирует руководство ответственного органа публичной власти о трудностях, рисках, несоответствиях или потребностях в содействии, выявленных во взаимодействии с управляющими.

39. Ответственный орган публичной власти информирует НЦКЗКИ о назначении или замене контактного пункта, а также об изменении его контактных данных в течение 5 рабочих дней с даты соответствующего изменения.

XII. УЧЕТ ОФИЦЕРОВ СВЯЗИ И ОБМЕН ИНФОРМАЦИЕЙ

40. Управляющий национальной критической инфраструктурой ведет внутренний учет офицеров связи, замещающих их лиц и соответствующих контактных

данных.

41. Ответственный орган публичной власти ведет учет офицеров связи, назначенных управляющими национальной критической инфраструктурой соответствующего сектора или подсектора.

42. Учет, предусмотренный пунктом 40, включает как минимум:

42.1. наименование управляющего;

42.2. наименование национальной критической инфраструктуры;

42.3. сектор и подсектор;

42.4. фамилию, имя и должность офицера связи;

42.5. служебные контактные данные;

42.6. фамилию, имя и должность замещающего его лица;

42.7. дату назначения;

42.8. дату обновления информации;

42.9. сведения об изменении или прекращении назначения.

43. Обмен информацией между управляющими, ответственными органами публичной власти и НЦКЗКИ осуществляется с соблюдением правового режима, применимого к передаваемой информации.

44. Информация об офицерах связи и контактных пунктах используется исключительно в целях сотрудничества в области защиты национальных критических инфраструктур.

45. Управляющий и ответственный орган публичной власти периодически, но не реже одного раза в год, проверяют актуальность контактных данных, должностей и статуса офицеров связи, замещающих их лиц и назначенных контактных пунктов и обеспечивают незамедлительное обновление соответствующих учетных данных в целях поддержания работоспособности механизмов уведомления, коммуникации и координации, в том числе в кризисных ситуациях.

XIII. ОБЩИЕ ПРАВИЛА ПРИМЕНЕНИЯ

И МЕТОДОЛОГИЧЕСКОГО СОГЛАСОВАНИЯ

46. Деятельность офицера связи по уведомлению, обмену информацией и оперативному взаимодействию осуществляется с соблюдением механизмов координации, коммуникации и отчетности, предусмотренных нормативной базой в области управления кризисными ситуациями и обеспечения непрерывности государственного управления, и без ущерба для таких механизмов.

47. Подробные обязанности офицера связи устанавливаются внутренним актом о назначении и, при необходимости, внутренними документами управляющего с соблюдением минимальных требований, предусмотренных настоящим приложением.

48. Назначение офицера связи не освобождает управляющего от установленных законом обязанностей в области защиты, безопасности, непрерывности, реагирования, восстановления и устойчивости национальной критической инфраструктуры.

49. Ответственные органы публичной власти могут разрабатывать секторальные инструкции или рекомендации по применению настоящего приложения с информированием НЦКЗКИ.

50. НЦКЗКИ может разрабатывать типовые образцы должностных обязанностей, реестров учета, форм уведомлений и другие методологические инструменты, необходимые для единообразного применения настоящего приложения.

51. Положения настоящего приложения применяются без ущерба для правового режима информации, отнесенной к государственной тайне, персональных данных, конфиденциальной информации и иных категорий информации, охраняемой законом.