



**Губернатор Ненецкого автономного округа**

**ПОСТАНОВЛЕНИЕ**

от 26 сентября 2022 г. № 62-пг  
г. Нарьян-Мар

**Об утверждении  
Положения о заместителе губернатора  
Ненецкого автономного округа, ответственном  
за обеспечение информационной безопасности  
в Администрации Ненецкого автономного округа**

В целях реализации Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», в соответствии с постановлением Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» ПОСТАНОВЛЯЮ:

1. Утвердить Положение о заместителе губернатора Ненецкого автономного округа, ответственном за обеспечение информационной безопасности в Администрации Ненецкого автономного округа, согласно Приложению.

2. Настоящее постановление вступает в силу со дня его официального опубликования.

Губернатор  
Ненецкого автономного округа



Ю.В. Безудный

Приложение  
к постановлению губернатора  
Ненецкого автономного округа  
от 26.09.2022 № 62-пг  
«Об утверждении Положения  
о заместителе губернатора Ненецкого  
автономного округа, ответственном  
за обеспечение информационной  
безопасности в Администрации  
Ненецкого автономного округа»

**Положение  
о заместителе губернатора Ненецкого  
автономного округа, ответственном за обеспечение  
информационной безопасности в Администрации  
Ненецкого автономного округа**

**Раздел I  
Общие положения**

1. Настоящее Положение определяет полномочия, права и обязанности заместителя губернатора Ненецкого автономного округа, ответственного за обеспечение информационной безопасности в Администрации Ненецкого автономного округа (далее – Администрация), в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты (далее – ответственное лицо).

2. Ответственное лицо определяется на основании распоряжения губернатора Ненецкого автономного округа.

3. Ответственное лицо осуществляет свою деятельность в соответствии с законом Ненецкого автономного округа от 06.01.2005 № 542-оз «Об Администрации Ненецкого автономного округа» на основе должностных обязанностей, утвержденных распоряжением губернатора Ненецкого автономного округа, с учетом особенностей деятельности Администрации и подчиняется непосредственно губернатору Ненецкого автономного округа.

4. Ответственное лицо входит в состав Администрации.

5. Указания и поручения ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми членами Администрации, государственными гражданскими служащими Ненецкого автономного округа и лицами, замещающими должности, не относящиеся к должностям государственной гражданской службы, в исполнительных органах Ненецкого автономного округа (далее – исполнительные органы).

**Раздел II  
Квалификационные требования к ответственному лицу**

6. Ответственное лицо должно иметь высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Если ответственное лицо имеет высшее образование по другому направлению подготовки (специальности), он должен пройти обучение по программе профессиональной переподготовки по направлению «Информационная безопасность».

7. Для ответственного лица требуются наличие следующих знаний, умений и профессиональных компетенций:

1) основные (в том числе производственные, бизнес и управленческие) процессы Администрации и специфика обеспечения информационной безопасности Администрации;

2) влияние информационных технологий на деятельность Администрации, в том числе:

роль и место информационных технологий (в том числе степень интеграции информационных технологий) в процессах функционирования Администрации;

зависимость основных процессов функционирования Администрации от информационных технологий;

3) информационно-телекоммуникационные технологии, в том числе:

современные информационно-телекоммуникационные технологии, используемые в Администрации;

способы построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления формирования информационных ресурсов (далее – системы и сети), в том числе ограниченного доступа;

типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами;

принципы построения и функционирования современных операционных систем, систем управления базами данных, систем и сетей, основных протоколов систем и сетей;

4) обеспечение информационной безопасности, в том числе:

цели, задачи, основы организации, ключевые элементы, основные способы и средства обеспечения информационной безопасности;

цели обеспечения информационной безопасности применительно к основным процессам функционирования Администрации, реализации и контроля их достижения;

принципы и направления стратегического развития информационной безопасности в Администрации;

правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Администрации, состав и содержание таких документов;

порядок организации работ по обеспечению информационной безопасности в Администрации;

основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности Администрации для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок

и контроля результативности применяемых способов и методов обеспечения информационной безопасности Администрации;

основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации, а также порядок оценки таких угроз;

возможности и назначения типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;

способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей;

порядок организации взаимодействия Администрации с исполнительными органами при решении вопросов обеспечения информационной безопасности;

управление проектами по информационной безопасности;

антикризисное управление и принятие управленческих решений при реагировании на кризисы и компьютерные инциденты;

планирование деятельности по обеспечению информационной безопасности в Администрации, исполнительных органах и подведомственных им организациях;

формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности Администрации, исполнительных органов и подведомственных им организаций;

организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности в Администрации, исполнительных органах и подведомственных им организациях (далее – политика);

внедрение политики;

организация контроля и анализа применения политики;

организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению информационной безопасности в Администрации, исполнительных органах и подведомственных им организациях;

поддержка и совершенствование деятельности по обеспечению информационной безопасности в Администрации, исполнительных органах и подведомственных им организациях;

организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в Администрации;

организация внедрения способов и средств для обеспечения информационной безопасности в Администрации, исполнительных органах и подведомственных им организациях;

организация мероприятий по анализу и контролю состояния информационной безопасности Администрации и модернизации (трансформации) процессов функционирования Администрации в целях обеспечения информационной безопасности в Администрации;

обеспечение информационной безопасности в ходе эксплуатации систем и сетей, а также при выводе их из эксплуатации;

организация мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы Администрации и реагированию на компьютерные инциденты;

организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в Администрации, исполнительных органах и подведомственных им организациях.

8. С учетом области и вида деятельности Администрации от ответственного лица требуется знание нормативных правовых актов Российской Федерации, методических документов, международных и национальных стандартов в области:

- 1) защиты государственной тайны;
- 2) защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных;
- 3) обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
- 4) обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;
- 5) создания и обеспечения безопасного функционирования государственных информационных систем и информационных систем в защищенном исполнении;
- 6) создания, обеспечения технических условий установки и эксплуатации средств защиты информации;
- 7) иных нормативных правовых актов и стандартов в области информационной безопасности.

### Раздел III

#### **Трудовые (должностные) обязанности ответственного лица**

9. Ответственное лицо принимает участие в формировании политики Администрации, отвечает за согласование стратегии развития Администрации в части вопросов обеспечения информационной безопасности.

10. Ответственное лицо организует:

1) разработку политики, направленной в том числе на обеспечение и поддержание стабильной деятельности Администрации и ее процессов функционирования в случае проведения компьютерных атак, отвечает за согласование и утверждение политики в Администрации, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики;

2) работу по обеспечению информационной безопасности Администрации, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, формулированию перечня негативных последствий, проведению мероприятий по их недопущению, отслеживанию и контролю эффективности (результативности) таких мероприятий, а также по необходимому информационному обмену;

3) реализацию и контроль проведения в Администрации организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю с учетом меняющихся угроз в информационной сфере, а также самостоятельно ответственным лицом в результате своей деятельности;

4) беспрепятственный доступ (в том числе удаленный) должностным лицам Федеральной службы безопасности Российской Федерации и ее территориальных органов к информационным ресурсам, принадлежащим Администрации либо используемым Администрацией, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет», в целях осуществления мониторинга их защищенности, а также работникам структурного

подразделения, обеспечивающего информационную безопасность Администрации и исполнительных органов;

5) взаимодействие с должностными лицами Федеральной службы безопасности Российской Федерации и ее территориальных органов, в том числе контроль исполнения указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами по результатам мониторинга защищенности информационных ресурсов, принадлежащих Администрации и исполнительным органам либо используемых Администрацией и исполнительными органами, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет»;

6) контроль за выполнением требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного порядка выполнения работ при решении вопросов, касающихся защиты информации;

7) развитие информационной безопасности, формирование и развитие навыков государственных гражданских служащих Ненецкого автономного округа и лиц, замещающих должности, не относящиеся к должностям государственной гражданской службы, в исполнительных органах в сфере информационной безопасности;

8) разработку и реализацию мероприятий по обеспечению информационной безопасности в Администрации и исполнительных органах в соответствии с требованиями к обеспечению информационной безопасности, установленными федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации;

9) контроль пользователей информационных ресурсов Администрации и исполнительных органов в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации;

10) планирование мероприятий по обеспечению информационной безопасности в Администрации, исполнительных органах и подведомственных им организациях;

11) подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Администрации и исполнительных органах, осуществляет согласование иных документов Администрации и исполнительных органов в части обеспечения информационной безопасности;

12) проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности в Администрации, исполнительных органах и подведомственных им организациях;

13) проведение контроля за состоянием обеспечения информационной безопасности в Администрации, исполнительных органах и подведомственных им организациях, включая оценку защищенности систем и сетей, оператором которых является Администрация, исполнительные органы и подведомственные им организации.

11. Ответственное лицо осуществляет:

1) регулярный контроль текущего уровня (состояния) информационной безопасности в Администрации и исполнительных органах, а также отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности в Администрации и исполнительных

органах, в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак;

2) регулярное и своевременное информирование губернатора Администрации Ненецкого автономного округа о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в Администрации и исполнительных органах и результатах практических учений по противодействию компьютерным атакам;

3) контроль за ведением организационно-распорядительной документации, статистического учета и отчетности по курируемым разделам работы;

4) согласование требований к системам и сетям, операторами которых являются Администрация, исполнительные органы и подведомственные им организации, в части обеспечения информационной безопасности;

5) руководство структурным подразделением, обеспечивающим информационную безопасность Администрации и исполнительных органов.

12. Ответственное лицо:

1) организует и контролирует проведение мероприятий по анализу и оценке состояния информационной безопасности Администрации и исполнительных органов и контролирует их результаты;

2) организует и контролирует функционирование системы обеспечения информационной безопасности в Администрации, координирует функционирование систем обеспечения информационной безопасности в исполнительных органах и подведомственных им организаций;

3) координирует деятельность исполнительных органов и подведомственных им организаций по вопросам обеспечения информационной безопасности.

13. Ответственное лицо согласовывает политику, технические задания и иную основополагающую документацию в сфере информационных технологий, цифровизации и цифровой трансформации Администрации и исполнительных органов.

14. Ответственное лицо с использованием нормативных правовых документов и методических материалов Федеральной службы безопасности Российской Федерации организует обнаружение, предупреждение и ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты с информационными ресурсами Администрации и исполнительных органов, а также взаимодействие с Национальным координационным центром по компьютерным инцидентам одним (или несколькими) из следующих способов:

силами структурного подразделения, обеспечивающего информационную безопасность Администрации и исполнительных органов, с заключением соглашения (издания совместного акта) о взаимодействии с Федеральной службой безопасности Российской Федерации (Национальным координационным центром по компьютерным инцидентам), включающего в том числе права и обязанности сторон, порядок проведения совместных мероприятий, регламент информационного обмена, порядок и сроки представления отчетности, порядок и формы контроля;

силами организаций, являющихся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

15. Ответственное лицо обеспечивает планирование и реализацию мероприятий по переводу систем и сетей на отечественные средства защиты информации, а также контроль за соблюдением запрета на использование средств

защиты информации, странами происхождения которых являются иностранные государства в соответствии с пунктом 6 Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

16. Ответственное лицо сопровождает мероприятия по разработке (модернизации) систем и сетей в части информационной безопасности, а также требований нормативных правовых актов, нормативно-технических и методических документов по защите информации и выполнения этих требований.

17. Ответственное лицо проводит работу по унификации способов и средств по обеспечению информационной безопасности, иных технических решений в Администрации, исполнительных органах и подведомственных им организациях.

18. Ответственное лицо принимает меры по совершенствованию обеспечения информационной безопасности в Администрации, исполнительных органах и подведомственных им организациях.

19. Ответственное лицо повышает на постоянной основе профессиональную компетенцию, знания и навыки в области обеспечения информационной безопасности.

20. Ответственное лицо выполняет иные обязанности, исходя из возложенных полномочий и поставленных губернатором Ненецкого автономного округа задач в рамках обеспечения информационной безопасности Администрации, исполнительных органов и подведомственных им организаций.

21. Ответственное лицо:

1) соблюдает и обеспечивает выполнение законодательства Российской Федерации;

2) в случаях, установленных законодательством Российской Федерации, согласовывает политику с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю;

3) представляет по запросам Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю достоверные сведения о результатах реализации политики (фактически достигнутом эффекте и результате) и текущем уровне (состоянии) информационной безопасности в Администрации;

4) организывает при необходимости проведение и участвует в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;

5) участвует в пределах компетенции в осуществлении закупок товаров, работ, услуг для обеспечения нужд в сфере информационной безопасности.

#### Раздел IV

#### Права ответственного лица

22. Ответственное лицо имеет право:

1) давать указания и поручения членам Администрации и руководителям исполнительных органов в части обеспечения информационной безопасности;



2) запрашивать от членов Администрации и руководителей исполнительных органов информацию и материалы, необходимые для реализации возложенных на ответственное лицо прав и обязанностей;

3) участвовать в заседаниях Администрации, принятии решений по вопросам деятельности Администрации и исполнительных органов, а также по внесению предложений по совершенствованию деятельности Администрации и исполнительных органов;

4) участвовать в разработке политики, выносить политику на заседание Администрации для обсуждения и утверждения;

5) представлять результаты реализации политики Администрации;

6) принимать решения по вопросам обеспечения информационной безопасности Администрации и исполнительных органов;

7) взаимодействовать с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и иными федеральными органами исполнительной власти по вопросам обеспечения информационной безопасности, в том числе по вопросам совершенствования законодательства Российской Федерации в области обеспечения информационной безопасности;

8) вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности;

9) инициировать проверки уровня (состояния) обеспечения информационной безопасности в Администрации, исполнительных органах и подведомственных им организациях;

10) организовывать на объектах Администрации мероприятия по информационной безопасности, разработку и представление губернатору Ненецкого автономного округа предложений по внесению изменений в процессы функционирования, принятию других мер, направленных на недопущение реализации негативных последствий;

11) получать доступ в установленном порядке к сведениям, составляющим государственную тайну, если исполнение обязанностей ответственного лица связано с использованием таких сведений и наличием необходимых прав и полномочий;

12) получать доступ в установленном порядке в связи с исполнением своих обязанностей в государственные органы Ненецкого автономного округа, органы местного самоуправления муниципальных образований Ненецкого автономного округа, общественные объединения и другие организации;

13) обеспечивать надлежащие организационно-технические условия, необходимые для исполнения обязанностей ответственного лица.

## Раздел V

### Ответственность ответственного лица

23. Ответственное лицо в соответствии с законодательством Российской Федерации несет ответственность:

1) за неисполнение или ненадлежащее исполнение своих обязанностей;

2) за действия (бездействие), ведущие к нарушению прав и законных интересов Администрации;

- 3) за разглашение государственной тайны и иных сведений, ставших ему известными в связи с исполнением своих обязанностей;
  - 4) за достижение целей обеспечения информационной безопасности;
  - 5) за поддержание и непрерывное развитие информационной безопасности Администрации для исключения (невозможности реализации) негативных последствий;
  - 6) за организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности Администрации;
  - 7) за нарушения требований по обеспечению информационной безопасности;
  - 8) за нарушения в обеспечении защиты систем и сетей, повлекшие негативные последствия.
-