Постановление Правительства Российской Федерации от 15.07.2022 г. № 1272
(Официальный интернет-портал правовой информации (www.pravo.gov.ru) от 19.07.2022 г., ст. 0001202207190035; Собрание законодательства Российской Федерации от 2022 г., № 30, ст. 5610)

Исходная редакция

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 15 июля 2022 г. № 1272

МОСКВА

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)

В соответствии с подпунктом "а" пункта 3 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" Правительство Российской Федерации постановляет:

Утвердить прилагаемые:

типовое положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации);

типовое положение о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации).

Председатель Правительства
Российской Федерации М.Мишустин

УТВЕРЖДЕНО
постановлением Правительства

Российской Федерации
от 15 июля 2022 г. № 1272

ТИПОВОЕ ПОЛОЖЕНИЕ
о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации)

I. Общие положения

1. Настоящее типовое положение определяет полномочия, права и обязанности заместителя руководителя федерального органа исполнительной власти, высшего исполнительного органа субъекта Российской Федерации, государственного фонда, государственной корпорации (компании) и иной организации, созданной на основании федерального закона, стратегического предприятия, стратегического акционерного общества и системообразующей организации российской экономики, юридического лица, являющегося субъектом критической информационной инфраструктуры Российской Федерации (далее - орган (организация), ответственного за обеспечение информационной безопасности в органе (организации), в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты (далее - ответственное лицо).

2. Ответственное лицо определяется руководителем органа (организации).

3. Ответственное лицо осуществляет свою деятельность на основе должностных регламентов (инструкций) федеральных государственных гражданских служащих и государственных гражданских служащих субъекта Российской Федерации, должностных инструкций работников организаций всех форм собственности с учетом особенностей деятельности органа (организации) (далее - работники органа (организации) и подчиняется непосредственно руководителю органа (организации) либо должностному лицу, его замещающему.

4. Ответственное лицо входит в состав коллегиальных органов органа (организации).

5. Указания и поручения ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми государственными служащими, муниципальными служащими и работниками органа (организации).

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:

а) основные (в том числе производственные, бизнес и управленческие) процессы органа (организации) и специфика обеспечения информационной безопасности органа (организации);

б) влияние информационных технологий на деятельность органа (организации), в том числе:

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

зависимость основных процессов функционирования органа (организации) от информационных технологий;

в) информационно-телекоммуникационные технологии, в том числе:

современные информационно-телекоммуникационные технологии, используемые в органе (организации);

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;

г) 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 органа (организации), реализации и контроля их достижения;

принципы и направления стратегического развития информационной безопасности в органе (организации);

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

порядок организации работ по обеспечению информационной безопасности в органе (организации);

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

применяемых способов и методов обеспечения информационной безопасности органа (организации);

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 структурных подразделений органа (организации) 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 органе (организации), подведомственных организациях (филиалах, представительствах);

формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности органа (организации), подведомственных организаций (филиалов, представительств);

организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности в органе (организации), в подведомственных организациях (филиалах, представительствах) (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 органе (организации), подведомственных организациях (филиалах, представительствах);

поддержка и совершенствование деятельности по обеспечению информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);

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

организация внедрения способов и средств для обеспечения информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);

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

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 органа (организации) и реагированию на компьютерные инциденты;

организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в органе (организации), подведомственных организациях (филиалах, представительствах).

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

а) защиты государственной тайны;

б) защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных;

в) обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

г) обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

д) создания и обеспечения безопасного функционирования государственных информационных систем и информационных систем в защищенном исполнении;

е) создания, обеспечения технических условий установки и эксплуатации средств защиты информации;

ж) иных нормативных правовых актов и стандартов в области информационной безопасности.

III. Трудовые (должностные) обязанности ответственного лица

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

10. Ответственное лицо:

а) организует разработку политики, направленной в том числе на обеспечение и поддержание стабильной деятельности органа (организации) и его (ее) процессов функционирования в случае проведения компьютерных атак, отвечает за согласование и утверждение политики в органе (организации), реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики;

б) организует работу по обеспечению информационной безопасности органа (организации), 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;

в) организует реализацию и контроль проведения в органе (организации) 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;

г) организует беспрепятственный доступ (в том числе удаленный) должностным лицам Федеральной службы безопасности Российской Федерации и ее территориальных органов к информационным ресурсам, принадлежащим органу (организации) либо используемым органом (организациями), доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет", в целях осуществления мониторинга их защищенности, а также работникам структурного подразделения, осуществляющего функции по обеспечению информационной безопасности;

д) организует 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 органу (организации) либо используемых органом (организациями), доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет";

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

ж) организует развитие информационной безопасности, формирование и развитие навыков работников органа (организации) в сфере информационной безопасности;

з) организует разработку и реализацию мероприятий по обеспечению информационной безопасности в органе (организации) в соответствии с требованиями к обеспечению информационной безопасности, установленными федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации;

и) организует контроль пользователей информационных ресурсов органа (организации) в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации;

к) организует планирование мероприятий по обеспечению информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);

л) организует подготовку правовых актов, иных организационно-распорядительных

документов по вопросам обеспечения информационной безопасности в органе (организации), осуществляет согласование иных документов органа (организации) в части обеспечения информационной безопасности;

м) организует проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах);

н) организует проведение контроля за состоянием обеспечения информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах), включая оценку защищенности систем и сетей, оператором которых является орган (организация), подведомственные организации (филиалы, представительства).

11. Ответственное лицо:

а) осуществляет регулярный контроль текущего уровня (состояния) информационной безопасности в органе (организации), а также отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности в органе (организации), в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак;

б) осуществляет регулярное и своевременное информирование руководства органа (организации) о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в органе (организации) и результатах практических учений по противодействию компьютерным атакам;

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

г) осуществляет согласование требований к системам и сетям, оператором которых является орган (организация), подведомственные организации (филиалы, представительства), в части обеспечения информационной безопасности;

д) осуществляет руководство структурным подразделением органа (организации), обеспечивающим информационную безопасность органа (организации).

12. Ответственное лицо:

а) организует и контролирует проведение мероприятий по анализу и оценке состояния информационной безопасности органа (организации) и контролирует их результаты;

б) организует и контролирует функционирование системы обеспечения информационной безопасности в органе (организации), координирует функционирование систем обеспечения информационной безопасности в подведомственных организациях (филиалах, представительствах);

в) координирует деятельность иных структурных подразделений органа (организации), подведомственных организаций (филиалов, представительств) по вопросам обеспечения информационной безопасности.

13. Ответственное лицо согласовывает политику, технические задания и иную

основополагающую документацию в сфере информационных технологий, цифровизации и цифровой трансформации органа (организации).

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 органа (организации), а также взаимодействие с Национальным координационным центром по компьютерным инцидентам одним (или несколькими) из следующих способов:

а) силами структурного подразделения, ответственного за обеспечение информационной безопасности, 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;

б) силами структурного подразделения, ответственного за обеспечение информационной безопасности, с его аккредитацией как центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

в) 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 "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 органе (организации), подведомственных организациях (филиалах, представительствах).

18. Ответственное лицо принимает меры по совершенствованию обеспечения информационной безопасности в органе (организации), подведомственных организациях (филиалах, представительствах).

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 руководством органа (организации) задач в рамках обеспечения информационной безопасности органа (организации), подведомственных организаций (филиалов, представительств).

21. Ответственное лицо:

а) соблюдает и обеспечивает выполнение законодательства Российской Федерации;

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

в) 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 органе (организации);

г) поддерживает уровень квалификации и постоянно развивает свои навыки в области информационной безопасности, необходимые для обеспечения информационной безопасности в органе (организации);

д) организовывает 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;

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

IV. Права ответственного лица

22. Ответственное лицо имеет право:

а) давать указания и поручения работникам органа (организации) в части обеспечения информационной безопасности;

б) запрашивать от работников органа (организации) информацию и материалы, необходимые для реализации возложенных на ответственное лицо прав и обязанностей;

в) участвовать в заседаниях (совещаниях) коллегиальных органов органа (организации), принятии решений по вопросам деятельности органа (организации), а также по внесению предложений по совершенствованию деятельности органа (организации);

г) участвовать в разработке политики, выносить политику на обсуждение, утверждение коллегиальному органу органа (организации);

д) представлять результаты реализации политики коллегиальному органу (органа) организации;

е) принимать решения по вопросам обеспечения информационной безопасности органа (организации);

ж) 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;

з) 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;

и) инициировать проверки уровня (состояния) обеспечения информационной безопасности в органе (организации), ее подведомственных и дочерних организациях;

к) организовывать на объектах органа (организации) мероприятия по информационной безопасности, разработку и представление руководителю органа (организации) предложений по внесению изменений в процессы функционирования, принятию других мер, направленных на недопущение реализации негативных последствий;

л) 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;

м) получать доступ в установленном порядке в связи с исполнением своих обязанностей в государственные органы, органы местного самоуправления, общественные объединения и другие организации;

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

V. Ответственность ответственного лица

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

а) за неисполнение или ненадлежащее исполнение своих обязанностей;

б) за действия (бездействие), ведущие к нарушению прав и законных интересов органа (организации);

в) за разглашение государственной тайны и иных сведений, ставших ему известными в связи с исполнением своих обязанностей;

г) за достижение целей обеспечения информационной безопасности;

д) за поддержание и непрерывное развитие информационной безопасности органа (организации) для исключения (невозможности реализации) негативных последствий;

е) за организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности органа (организации);

ж) за нарушения требований по обеспечению информационной безопасности;

з) за нарушения в обеспечении защиты систем и сетей, повлекшие негативные последствия.

_____

УТВЕРЖДЕНО
постановлением Правительства
Российской Федерации
от 15 июля 2022 г. № 1272

ТИПОВОЕ ПОЛОЖЕНИЕ
о структурном подразделении органа (организации), обеспечивающем информационную безопасность органа (организации)

I. Общие положения

1. Настоящее типовое положение определяет цели, задачи и функции структурного подразделения федерального органа исполнительной власти, высшего исполнительного органа субъекта Российской Федерации, государственного фонда, государственной корпорации (компании) и иной организации, созданной на основании федерального закона, стратегического предприятия, стратегического акционерного общества и системообразующей организации российской экономики, юридического лица, являющегося субъектом критической информационной инфраструктуры Российской Федерации (далее - орган (организация), обеспечивающего информационную безопасность органа (организации) (далее - подразделение).

2. Подразделение в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, другими нормативными правовыми документами в сфере обеспечения информационной безопасности, указаниями руководителя органа (организации) и настоящим типовым положением.

3. Подразделение подчинено заместителю руководителя органа (организации), ответственному за обеспечение информационной безопасности в органе (организации), либо иным лицам из состава руководства органа (организации) при условии осуществления курирования со стороны руководителя органа (организации).

4. Контроль за деятельностью подразделения осуществляет руководитель органа

(организации).

II. Цели и задачи деятельности подразделения

5. Деятельность подразделения направлена:

а) на исключение или существенное снижение негативных последствий (ущерба) в отношении органа (организации) вследствие нарушения функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления в результате реализации угроз безопасности информации;

б) на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

в) на повышение защищенности органа (организации) от возможного нанесения ему (ей) материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем органа (организации) или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования;

г) на обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры органа (организации);

д) на обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем и информационно-телекоммуникационной инфраструктуры органа (организации).

6. Основными задачами деятельности подразделения являются:

а) планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в органе (организации);

б) выявление угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств;

в) предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

г) поддержание стабильной деятельности органа (организации) и его (ее) производственных процессов в случае проведения компьютерных атак;

д) взаимодействие с Национальным координационным центром по компьютерным инцидентам;

е) обеспечение нормативно-правового обеспечения использования информационных ресурсов.

III. Функции подразделения

7. Подразделение выполняет следующие функции:

а) разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в органе (организации) и подведомственных органах (организациях);

б) разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в органе (организации) и представление их руководителю органа (организации);

в) выявление и проведение анализа угроз безопасности информации в отношении органа (организации), уязвимостей информационных систем, программного обеспечения программно-аппаратных средств и принятие мер по их устранению;

г) обеспечение в соответствии с требованиями по информационной безопасности, в том числе с целью исключения (невозможности реализации) негативных последствий, разработки и реализации организационных мер и применения средств обеспечения информационной безопасности;

д) обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;

е) представление в Национальный координационный центр по компьютерным инцидентам информации о выявленных компьютерных инцидентах;

ж) исполнение указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами, Федеральной службой по техническому и экспортному контролю по результатам мониторинга защищенности информационных ресурсов, принадлежащих органу (организации) либо используемых органом (организацией), доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет";

з) проведение анализа и контроля за состоянием защищенности систем и сетей и разработка предложений по модернизации (трансформации) основных процессов органа (организации) в целях обеспечения информационной безопасности в органе (организации);

и) подготовка отчетов о состоянии работ по обеспечению информационной безопасности в органе (организации);

к) организация развития навыков безопасного поведения в органе (организации), в том числе проведение занятий с руководящим составом и специалистами органа (организации) по вопросам обеспечения информационной безопасности;

л) выполнение иных функций, исходя из поставленных руководством органа (организации) целей и задач в рамках обеспечения информационной безопасности в органе (организации), подведомственных органах (организациях).

IV. Права подразделения

8. С целью реализации функций подразделение имеет право:

а) запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений органа (организации), необходимым для принятия решений по всем вопросам, отнесенным к компетенции подразделения;

б) готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности организаций, имеющих лицензии на соответствующий вид деятельности;

в) контролировать деятельность любого структурного подразделения органа (организации) по выполнению требований к обеспечению информационной безопасности;

г) постоянно повышать профессиональные компетенции, знания и навыки работников в области обеспечения информационной безопасности;

д) участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;

е) участвовать в работе комиссий органа (организации) при рассмотрении вопросов обеспечения информационной безопасности;

ж) вносить предложения руководству органа (организации) о приостановлении работ в случае обнаружения факта нарушения информационной безопасности;

з) вносить представления руководству органа (организации) в отношении государственных служащих, муниципальных служащих и работников органа (организации) (далее - работники) при обнаружении фактов нарушения работниками установленных требований безопасности информации в органе (организации), в том числе ходатайствовать о привлечении указанных работников к административной или уголовной ответственности;

и) вносить на рассмотрение руководству органа (организации) предложения по вопросам деятельности подразделения.

V. Взаимоотношения и связи подразделения

9. Подразделение осуществляет свои полномочия во взаимодействии со структурными подразделениями органа (организации) и подведомственными ему органами (организациями), а также в пределах своей компетенции с иными органами (организациями) и гражданами в установленном порядке.

10. По указанию руководства осуществляет взаимодействие с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации по вопросам информационной безопасности.

VI. Показатели эффективности и результативности подразделения

11. Эффективность и результативность деятельности подразделения определяются по итогам выполнения органом (организацией), а также подведомственными ему органами (организациями) программы обеспечения информационной безопасности с учетом приоритетных целей, предусмотренных разделом II настоящего типового положения.

12. Работники подразделения несут ответственность за выполнение возложенных на них обязанностей в соответствии с должностными регламентами, утверждаемыми руководителем органа (организации) либо должностным лицом, наделенным руководителем органа (организации) соответствующими полномочиями.