**Санкт-Петербургское государственное УТВЕРЖДАЮ:**

**бюджетное учреждение здравоохранения** Директор

**«Медицинский информационно**

**-аналитический центр»** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /А.В.Язенок/

**(СПб ГБУЗ МИАЦ)** «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

**заместителя директора, ответственного**

**за обеспечение информационную безопасность ( в дальнейшем –ИБ)**

**в организации – далее заместитель директора по ИБ**

1. **Общие положения**

1.1.Заместителя директора, ответственного за обеспечение информационной безопасности в СПб ГБУЗ МИАЦ в (дальнейшем – организации) – далее заместитель директора по ИБ относится к категории руководителей.

1*.* 2. На должность заместитель директора по ИБ назначается лицо, имеющее:

– высшего профессионального образования по направлению подготовки (специальности) в области ИБ или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе профессиональной переподготовки по направлению "Информационная безопасность";

- наличие стажа работы в сфере ИБ не менее 3 лет;

1.3. Назначение на должность заместитель директора по ИБ и освобождение от нее производится приказом директора орпганизации.

1.4. Заместитель директора по ИБ осуществляет свою деятельность на основе данной должностной инструкции и подчиняется непосредственно директору организации либо должностному лицу, его замещающему.

1.5. Заместитель директора по ИБ входит в состав коллегиальных органов организации, ответственных за организацию и контроль выполнения требований государственных органов и организаций, которые устанавливают, контролируют и обеспечивают соблюдение нормативных правовых актов, стандартов и требований в сфере ИБ законодательства (в дальнейшем – регуляторов по ИБ) в организации.

1.6. Указания и поручения заместитель директора по ИБ, в части обеспечения информационной безопасности, обязательны для исполнения всеми сотрудниками организации.

1.7. Заместитель директора по ИБ должно обладать следующими знаниями, умениями и профессиональными компетенциями:

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

б) влияние информационных технологий (в дальнейшем – ИТ) на деятельность организации, в том числе:

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

- зависимость основных процессов функционирования 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 ИБ, в том числе:

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

- цели обеспечения ИБ применительно к основным процессам функционирования организации, реализации и контроля их достижения;

- принципы и направления стратегического развития ИБ в организации;

- правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения ИБ в организации, состав и содержание таких документов;

- порядок организации работ по обеспечению ИБ в организации;

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

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

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

- способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей, взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее - ГосСОПКА);

- порядок организации взаимодействия структурных подразделений организации при решении вопросов обеспечения ИБ;

- разработкой, обоснования и управление проектами по ИБ в организации;

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

- планирование деятельности по обеспечению ИБ в организации, подведомственных организациях (филиалах, представительствах);

- формулирование измеримых и практических результатов деятельности по обеспечению ИБ организации);

- организация разработки, утверждения, внедрение политики и контроля и анализа применения (правил, процедур), регламентирующей вопросы ИБ в организации (далее – политика);

- организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению ИБ в организации;

- поддержка и совершенствование деятельности по обеспечению ИБ в организации;

- организация мероприятий (актуализации по мере смены рекомендаций ГосСОПКА) по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению ИБ в организации;

- организация внедрения способов и средств для обеспечения ИБ в организации;

- организация мероприятий по анализу и контролю состояния ИБ организации и модернизации (трансформации) процессов функционирования организации в целях обеспечения ИБ в организации;

- обеспечение ИБ 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 организации и реагированию на компьютерные инциденты;

- организация мероприятий по отслеживанию и контролю достижения целей ИБ (фактически достигнутый эффект и результат) в организации.

1. **Служебные обязанности заместителя директора по ИБ**

2.1 Заместитель директора по ИБ принимает участие в формировании политики органа (организации), отвечает за согласование стратегии развития организациив части вопросов обеспечения ИБ.

2.2. Заместителя директора по ИБ организует:

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

б) работу по обеспечению ИБ в 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, взаимодействия с ГосСОПКА;

в) организует реализацию и контроль проведения в организации организационных и технических мер, решения о необходимости осуществления которых принимаются ФСБ, ГосСОПКА и ФСТЭК 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 ФСБ и ее территориальных органов к информационным ресурсам, принадлежащим организации либо используемым 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 ИБ;

д) организует взаимодействие с должностными лицами ФСБ и ее территориальных органов, в том числе контроль исполнения указаний, данных ФСБ 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 ИБ в организации;

ж) Организует развитие ИБ в организации, планирует и контролирует занятия по формированию и развитию навыков работников в сфере ИБ.

з) организует разработку и реализацию мероприятий по обеспечению информационной безопасности в организации в соответствии с требованиями к обеспечению ИБ, установленными регуляторами по ИБ и рекомендациями ГосСОПКА;

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

к) организует планирование мероприятий по обеспечению ИБ в организации;

л) организует подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения ИБ в организации, осуществляет согласование иных документов организации в части обеспечения ИБ;

м) организует проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности в организации (данное требование указано только в пост. Прав. 1272);

н) организует проведение контроля за состоянием обеспечения информационной безопасности в организации, включая оценку защищенности систем и сетей, оператором которых является организация.

11. Заместителя директора по ИБ осуществляет:

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

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

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

г) согласование требований к системам и сетям, оператором которых является организация, в части обеспечения информационной безопасности;

д) руководство структурным подразделением организации, обеспечивающим информационную безопасность организации.

12. Заместителя директора по ИБ организует и контролирует:

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

13. Заместитель директора по ИБ согласовывает политику, технические задания и иную основополагающую документацию в сфере информационных технологий, цифровизации и цифровой трансформации органа (организации).

14. Заместитель директора по ИБ с использованием нормативных правовых документов и методических материалов ФСБ организует обнаружение, предупреждение и ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты с информационными ресурсами организации, а также взаимодействие с ГосСОПКА.

15. Заместитель директора по ИБ 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](https://base.garant.ru/404561984/a1cb606166e1375dd552747a8ff016cc/#block_6) Указа Президента Российской Федерации "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".

16. Заместитель директора по ИБ сопровождает мероприятия по разработке (модернизации) систем и сетей в части ИБ, а также требований регуляторов по ИБ.

17. Заместитель директора по ИБ проводит работу по унификации способов и средств по обеспечению информационной безопасности, иных технических решений в организации.

18. Заместитель директора по ИБ принимает меры по совершенствованию обеспечения информационной безопасности в организации.

19. Заместитель директора по ИБ повышает профессиональную компетенцию, знания и навыки в области обеспечения информационной безопасности (повышение квалификации не реже 1 раза в 3 года).

20. Заместитель директора по ИБ выполняет иные обязанности, исходя из возложенных полномочий и поставленных руководством организации задач в рамках обеспечения информационной безопасности организации.

21. Заместитель директора по ИБ:

а) соблюдает и обеспечивает выполнение законодательства Российской Федерации;

б) в случаях, установленных законодательством Российской Федерации, согласовывает политику с ФСБ и ФСТЭК;

в) представляет по запросам ФСБ и ФСТЭК достоверные сведения о результатах реализации политики (фактически достигнутом эффекте и результате) и текущем уровне (состоянии) информационной безопасности в 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.

22 Заместитель директора по ИБ должен знать:

- Нормативно-правовые акты, методические руководства и нормативные материалы, регламентирующие область ИБРФ для СПб ГБУЗ МИАЦ, включая документацию и техническое обеспечение защиты информации.;

- особенности деятельности СПб ГБУЗ МИАЦ;

- правила внутреннего распорядка;

- правила и нормы охраны труда и пожарной безопасности.

**IV. Права ответственного лица**

1. Заместитель директора по ИБ имеет право:

а) Давать указания и поручения сотрудникам организации в части обеспечения информационной безопасности.

б) Запрашивать и получать необходимую для работы информацию от сотрудников организации.

в) Участвовать в заседаниях и совещаниях коллегиальных органов организации по вопросам ИБ.

г) Представлять результаты реализации политики информационной безопасности. д) Взаимодействовать с государственными органами и другими организациями по вопросам информационной безопасности.

**V. Ответственность**

1. Заместитель директора по ИБ несет ответственность:

а) За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных данной инструкцией, в порядке, установленном действующим трудовым законодательством Российской Федерации.

б) За правонарушения и преступления, совершенные в процессе своей деятельности, в порядке, установленном действующим административным, уголовным и гражданским законодательством Российской Федерации. Приложение № 1

в) За причинение материального ущерба, в порядке, установленном действующим трудовым законодательством Российской Федерации.