Приложение № 1
К Приказу № 133с
от «17» 03 2023г.

ПОЛОЖЕНИЕ
О ЗАМЕСТИТЕЛЕ ГЛАВНОГО ВРАЧА ОБУЗ «ГКБ №3 г. Иванова», ОТВЕТСТВЕННЫМ ЗА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИИ

I. Общие положения

1. Настоящее Положение определяет полномочия, права и обязанности заместителя главного врача ОБУЗ «ГКБ №3 г. Иванова» (далее - Учреждение), ответственного за обеспечение информационной безопасности в Учреждении, в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты (далее - ответственное лицо).

2. Ответственное лицо определяется главным врачом (руководителем) Учреждения.

3. Ответственное лицо осуществляет свою деятельность на основе должностной инструкции с учетом особенностей деятельности Учреждения и подчиняется непосредственно главному врачу (руководителю) Учреждения либо должностному лицу, его замещающему.

4. Ответственное лицо входит в состав коллегиальных органов Учреждения.

5. Указания и поручения ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми работниками Учреждения

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 Учреждения и специфика обеспечения информационной безопасности Учреждения;

б) влияние информационных технологий на деятельность Учреждения, в том числе:

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

зависимость основных процессов функционирования Учреждения от информационных технологий;

в) информационно-телекоммуникационные технологии, в том числе:

современные информационно-телекоммуникационные технологии, используемые в Учреждении;

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 Учреждения, реализации и контроля их достижения;

принципы и направления стратегического развития информационной безопасности в Учреждении;

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

порядок организации работ по обеспечению информационной безопасности в Учреждении;

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

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 Учреждения 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 Учреждении;

формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности Учреждения;

организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности в Учреждении (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 Учреждении;

поддержка и совершенствование деятельности по обеспечению информационной безопасности в Учреждении;

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

организация внедрения способов и средств для обеспечения информационной безопасности в Учреждении;

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

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 Учреждения и реагированию на компьютерные инциденты;

организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) Учреждении;

8. С учетом области и вида деятельности Учреждения 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 Учреждения, отвечает за согласование стратегии развития Учреждения в части вопросов обеспечения информационной безопасности.

10. Ответственное лицо:

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

б) организует работу по обеспечению информационной безопасности Учреждения, 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 Учреждении 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 системному администратору Учреждения, осуществляющему 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 Учреждению либо используемых им, 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 Учреждения в сфере информационной безопасности;

з) организует разработку и реализацию мероприятий по обеспечению информационной безопасности в Учреждении 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 Учреждения 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 Учреждении;

л) организует подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Учреждении, осуществляет согласование иных документов Учреждения в части обеспечения информационной безопасности;

м) организует проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности в Учреждении;

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

11. Ответственное лицо:

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

б) осуществляет во взаимодействии с системным администратором Учреждения регулярное и своевременное информирование руководства Учреждения 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 во взаимодействии с системным администратором Учреждения согласование требований к системам и сетям, оператором которых является Учреждение, в части обеспечения информационной безопасности;

д) осуществляет взаимодействие с системным администратором Учреждения, непосредственно обеспечивающим информационную безопасность Учреждения.

12. Ответственное лицо:

а) организует и контролирует во взаимодействии с системным администратором Учреждения проведение мероприятий по анализу и оценке состояния информационной безопасности органа (организации) и контролирует их результаты;

б) организует и контролирует во взаимодействии с системным администратором Учреждения функционирование системы обеспечения информационной безопасности в Учреждении, координирует функционирование систем обеспечения информационной безопасности в структурных подразделениях Учреждения;

в) во взаимодействии с системным администратором Учреждения координирует деятельность иных структурных подразделений Учреждения, по вопросам обеспечения информационной безопасности.

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

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

а) системным администратором, непосредственно ответственным 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 организаций, являющихся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

15. Ответственное лицо во взаимодействии с системным администратором Учреждения 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 п. 6 Указа Президента Российской Федерации "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".

16. Ответственное лицо во взаимодействии с системным администратором Учреждения 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 во взаимодействии с системным администратором Учреждения проводит работу по унификации способов и средств по обеспечению информационной безопасности, иных технических решений в Учреждении.

18. Ответственное лицо во взаимодействии с системным администратором Учреждения принимает меры по совершенствованию обеспечения информационной безопасности в Учреждении.

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 Учреждения задач в рамках обеспечения информационной безопасности Учреждения.

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) во взаимодействии с системным администратором Учреждения 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 Учреждении;

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

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

е) во взаимодействии с системным администратором Учреждения 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 Учреждения в части обеспечения информационной безопасности;

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

в) участвовать в заседаниях (совещаниях) коллегиальных органов Учреждения, 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 Учреждения;

д) представлять результаты реализации политики коллегиальному органу Учреждения;

е) принимать решения по вопросам обеспечения информационной безопасности Учреждения;

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 Учреждении;

к) организовывать на объектах Учреждения мероприятия по информационной безопасности, разработку и представление руководителю Учреждения 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 Учреждения для исключения (невозможности реализации) негативных последствий;

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

ж) за нарушения требований по обеспечению информационной безопасности;

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