Приложение № 2
К Приказу № 133а
от «27» 03 2023г.

ПОЛОЖЕНИЕ
О ДОЛЖНОСТНОМ ЛИЦЕ ОБУЗ «ГКБ №3 г. Иванова», ОТВЕТСТВЕННОМ ЗА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИИ

I. Общие положения

1. Настоящее положение определяет цели, задачи и функции должностного лица ОБУЗ «ГКБ №3 г. Иванова» (далее – Учреждение), являющегося субъектом критической информационной инфраструктуры Российской Федерации, обеспечивающего информационную безопасность Учреждения.

2. Должностным лицом, обеспечивающим информационную безопасность Учреждения, является инженер-программист Учреждения (далее – должностное лицо).

3. Должностное лицо в своей деятельности руководствуется Конституцией Рссийской 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 Учреждения и настоящим положением.

4. Должностное лицо по вопросам информационной безопасности подчинено заместителю главного врача (руководителя) Учреждения, ответственному за обеспечение информационной безопасности в Учреждении, либо иным лицам из состава руководства Учреждения при условии осуществления курирования со стороны главного врача (руководителя) Учреждения.

5. Контроль (курирование) за деятельностью должностного лица осуществляет главный врач (руководитель) Учреждения.

II. Цели и задачи деятельности должностного лица

5. Деятельность должностного лица направлена:

а) на исключение или существенное снижение негативных последствий (ущерба) в отношении Учреждения 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 Учреждения от возможного нанесения ему материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем Учреждения 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 Учреждения;

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

6. Основными задачами деятельности должностного лица являются:

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

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 Учреждения и его производственных процессов в случае проведения компьютерных атак;

д) взаимодействие с Департаментом здравоохранения Ивановской области и через него с Национальным координационным центром по компьютерным инцидентам;

е) обеспечение нормативно-правового обеспечения использования информационных ресурсов.

III. Функции должностного лица

7. Должностное лицо выполняет следующие функции:

а) разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в Учреждении;

б) разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в Учреждении и их согласование с Департаментом здравоохранения Ивановской области;

в) выявление и проведение анализа угроз безопасности информации в отношении Учреждения, 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 Департамент здравоохранения Ивановской области и через него 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, Департамента здравоохранения Ивановской области принадлежащих Учреждению либо используемых Учреждением, 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 в Учреждении в целях обеспечения информационной безопасности Учреждения с последующим сообщением в Департамент здравоохранения Ивановской области;

и) подготовка отчетов о состоянии работ по обеспечению информационной безопасности в Учреждении;

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

л) выполнение иных функций, исходя из поставленных руководством Учреждения целей и задач в рамках обеспечения информационной безопасности в Учреждении.

IV. Права должностного лица

8. С целью реализации функций должностное лицо имеет право:

а) запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений Учреждения, 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 Учреждения 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 выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ;

е) участвовать в работе комиссий Учреждения при рассмотрении вопросов обеспечения информационной безопасности;

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

з) вносить представления руководству Учреждения в отношении работников Учреждения (далее - работники) при обнаружении фактов нарушения работниками установленных требований безопасности информации в Учреждении, в том числе ходатайствовать о привлечении указанных работников к административной или уголовной ответственности;

и) вносить на рассмотрение руководству Учреждения предложения по вопросам своей деятельности.

V. Взаимоотношения и связи должностного лица

9. Должностное лицо осуществляет свои полномочия во взаимодействии со структурными подразделениями Учреждения, 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, а также Департаментом здравоохранения Ивановской области по вопросам информационной безопасности.

VI. Показатели эффективности и результативности должностного лица

11. Эффективность и результативность деятельности должностного лица определяются по итогам выполнения Учреждением программы обеспечения информационной безопасности с учетом приоритетных целей, предусмотренных разделом II настоящего положения.

12. Должностное лицо несет ответственность за выполнение возложенных на него обязанностей в соответствии с должностной инструкцией, утвержденной руководителем Учреждения либо должностным лицом, наделенным руководителем Учреждения соответствующими полномочиями.