ПРИКАЗ № 2026/01/20
по обществу с ограниченной ответственностью «Лечебный диагностический центр Международного института биологических систем - Калининград»

г. Калининград 20 января 2026 года

Об утверждении политики
информационной безопасности в
ООО «ЛДЦ МИБС-Калининград»

Во исполнение Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 N 152- ФЗ «О персональных данных» и иных нормативных правовых актов Российской Федерации,

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности в ООО «ЛДЦ МИБС Калининград» (далее — Политика) согласно Приложению № 1 к настоящему Приказу.
2. Главного бухгалтера ознакомить под расписку работников ООО «ЛДЦ МИБС-Калининград» с Политикой.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор Фимушкина Е.В.

СОГЛАСОВАНО:

Главный бухгалтер Теплова Т.В.

Приложение № 1
к приказу по ООО «ЛДЦ МИБС - Калининград» от 20.01.2026
№ 2026/01/20

ПОЛИТИКА

информационной безопасности в ООО «ЛДЦ МИБС - Калининград»

1. Термины и определения

1.1. **Бизнес-процесс** — последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Организации.

1.2. **Защита информации** — совокупности организационных и технический мер, направленных на предотвращение утечки защищаемой информации, несанкционированных и неправомерных воздействий на защищаемую информацию и средства доступа к ней.

1.3. **Информация** — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

1.4. **Информационная безопасность** — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, записи или уничтожения информации.

1.5. **Информационная система** — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.6. **Информационный ресурс** — все, что имеет ценность и находится в распоряжении Организации.

1.7. **Коммерческая тайна** — конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы и избежать неоправданные расходы, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

1.8. **Конфиденциальная информация** — информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

1.9. **Конфиденциальность информации** — состояние защищенности информации, характеризуемое способностью информационной системы обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

1.10. **Несанкционированный доступ** — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

1.11. **Политика** - общие цели и указания, формально выраженные руководством.

- Приказа ФСТЭК России от 25.12.2017 N 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказа ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

2.5. Применение СУИБ регламентировано настоящей Политикой, а также другими организационно-распорядительными документами (далее — ОРД) Организации, которые являются обязательными для исполнения всеми работниками Организации. Требования СУНБ доводятся до сведения работников Организации.

3. Цели и задачи

3.1. Основной целю настоящей Политики является защита ИС и ИР Организации от возможного нанесения им материального, физического, морального или иного ущерба, а также нарушения режима конфиденциальности информации в результате несанкционированного доступа к информации, ее носителям, а также процессам обработки и передачи информации.

3.2. Для достижения указанных целей СУИБ должна обеспечивать выполнение следующих задач:

- соответствие требованиям Федерального законодательства, нормативно-методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ;
- своевременное выявление, оценка и прогнозирование источников угроз НБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- достижение адекватности мер по защите от угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;
- обеспечение непрерывности критических бизнес-процессов;
- изучение партнеров, клиентов, конкурентов и кандидатов на работу;

5. Заключение

4.10. Настоящая Политика является внутренним документом Организации, общедоступной и подлежит размещению на официальном сайте Организации.

4.11. Настоящая Политика распространяется на все бизнес-процессы, автоматизированные и телекоммуникационные системы Организации.

4.12. Разработка внутренних организационно-распорядительных документов Организации, регламентирующих вопросы ИБ, осуществляется на основании настоящей Политикой.

4.13. Работники Организации должны руководствоваться настоящей Политикой в профессиональной деятельности, при внутрикорпоративном взаимодействии, личном развитии и повышении культуры ИБ.

4.14. Ответственность должностных лиц Организации, имеющих доступ к конфиденциальной информации, за невыполнение требований норм, регулирующих обработку и защиту информации, определяется в соответствии с законодательством Российской Федерации и внутренними организационно-распорядительными документами Организации.

4.15. Настоящая Политики вступает в силу с момента ее утверждения.