ПРИКАЗ № 21-2023
по обществу с ограниченной ответственностью «Лечебно-диагностический центр Международного института биологических систем имени Сергея Березина»

г. Санкт-Петербург 28 июля 2023 года

Об утверждении Политики информационной безопасности в ООО «ЛДЦ МИБС»

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

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности в ООО «ЛДЦ МИБС» (далее – Политика) согласно Приложению №1 к настоящему Приказу.
2. Руководителям структурных подразделений ознакомить под расписку работников ООО «ЛДЦ МИБС» с Политикой.
3. Контроль за исполнением настоящего приказа возложить на заместителя генерального директора по безопасности Смирнова Д.С.

Генеральный директор М.М. Архипкина

СОГЛАСОВАНО:

Заместитель генерального директора по безопасности Д.С. Смирнов

Приложение № 1
к приказу по ООО «ЛДЦ МИБС»
от 28.07.2023 № 21-2023

ПОЛИТИКА

информационной безопасности в ООО «ЛДЦ МИБС»

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, 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 иди 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.

1.12. **Права доступа** – это права доверенного объекта на совершение каких-либо действий по отношению к объектам системы.

1.13. **Риск** – сочетание вероятности события и его последствий.

1.14. **Система управления информационной безопасностью** – часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

1.15. **Угроза** – опасность, предполагающая возможность потерь (ущерба).

1.16. **Целостность информации** – устойчивость информации к несанкционированному доступу или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

2. Общее положение

2.1. Настоящая политика информационной безопасности (далее – Политика) Общества с ограниченной ответственностью «Лечебно-диагностический центр Международного института биологических систем имени Сергея Березина» (далее – Организация) представляет собой систему требований, правил и методов Организации в области обеспечения безопасности информации, ее конфиденциальности, а также построения системы управления информационной безопасностью (далее – СУИБ) Организации.

2.2. Соблюдение принципов, правил и требований информационной безопасности (далее – ИБ) является, в том числе, элементом корпоративной культуры. Следование требованиям ИБ является важным условием при осуществлении повседневной деятельности Организации, включая совместную работу с деловыми партнерами. Каждый работник Организации и ее деловые партнеры несут ответственность за безопасную работу с информационными системами (далее – ИС), информационными ресурсами (далее – ИР), компьютерным оборудованием, мобильными техническими средствами, носителями информации, предоставленной и обрабатываемой информацией Организации.

2.3. Обеспечение ИБ включает в себя любую деятельность, установленную действующим законодательством Российской Федерации, направленную на защиту ИС и ИР Организации.

2.4. Настоящая Политика разработана на основе требований законодательства Российской Федерации:

- Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных;
- Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи»;
- Федерального закона от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

- 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 СУИБ 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 ИБ;
- 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;

- недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
- повышение деловой репутации и корпоративной культуры в сфере ИБ.

4. Методы обеспечения информационной безопасности

4.1. Назначение и подготовка работников, ответственных за организацию и осуществление мероприятий по обеспечению ИБ.

4.2. Регламентирование всех процессов обработки информации, действий работников Организации и специалистов, осуществляющих администрирование программных и технических средств обработки информации, на основе утвержденной ОРД по вопросам обеспечения ИБ.

4.3. Учет всех, подлежащих защите, ИР (каналов связи, аппаратных и программных средств).

4.4. Предоставление каждому пользователю ИС минимально необходимых прав доступа для выполнения своих функциональных обязанностей.

4.5. Знание и строгое соблюдение всеми работниками, использующих и обслуживающих аппаратные и программные средства обработки информации, требований ОРД по вопросам обеспечения безопасности конфиденциальной информации, в том числе коммерческой тайны и критических бизнес-процессов.

4.6. Персональная ответственность за свои действия каждого работника, участвующего, в рамках своих функциональных обязанностей, в процессах обработки информации и имеющего доступ к ИР.

4.7. Реализация технологических процессов обработки информации в соответствии с комплексом организационно-технических мер по защиты программного обеспечения, технических средств и данных.

4.8. Принятие мер по обеспечению физической целостности технических средств ИС и поддержанием необходимого уровня защищенности их компонентов.

4.9. Использование физических и технических (программно-аппаратных) средств защиты информации (далее – СЗИ), а также техническая поддержка их использования.

4.10. Контроль соблюдения пользователями ИС требований по обеспечению ИБ.

4.11. Правовая защита интересов Организации при взаимодействии с юридическими и физическими лицами от противоправных и несанкционированных действий со стороны этих лиц.

4.12. Проведение анализа эффективности принятых мер и применяемых СЗИ. Разработка и реализация предложений по совершенствованию СУИБ в Организации.

4.13. Своевременное выявление источников угроз ИБ, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы ИБ.

4.14. Создание условий для минимизации наносимого ущерба неправомерными действиями, ослабление негативного влияния и устранения последствий нарушения ИБ.

5. Заключение

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

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

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

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

5.5. 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.

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