ФЕДЕРАЛЬНОЕ МЕДИКО-БИОЛОГИЧЕСКОЕ АГЕНТСТВО
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
ЮЖНО-УРАЛЬСКИЙ ИНСТИТУТ БИОФИЗИКИ
(ФГУП ЮУрИБФ)

ПРИКАЗ

05.02.2019 № 7

Об организации работ с персональными данными

г. Озёрск

Руководствуясь Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказом ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», в целях защиты персональных данных, обрабатываемых на предприятии,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с даты подписания настоящего Приказа Политику информационной безопасности.
2. Разместить текст документа на сайте ФГУП ЮУрИБФ. – Отв. Арутюнян О.Г.

Директор С.А.Романов

ФЕДЕРАЛЬНОЕ МЕДИКО-БИОЛОГИЧЕСКОЕ АГЕНТСТВО

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ

ЮЖНО-УРАЛЬСКИЙ ИНСТИТУТ БИОФИЗИКИ

(ФГУП ЮУрИБФ)

УТВЕРЖДАЮ

Директор ФГУП ЮУрИБФ

_____С.А. Романов

_____._____2019 г.

Политика информационной безопасности

Введено приказом № _____

от _____._____ 2019 г.

Срок действия

с _____._____2019 г.

до переиздания

1. Общие положения

1.1. Федеральное Государственное унитарное предприятие Южно-Уральский институт биофизики Федерального медико-биологического агентства (ФГУП ЮУрИБФ) – научно-исследовательская организация, основным видом деятельности которой являются научные исследования и разработки в области естественных и технических наук с целью получения новых научных знаний в области естественных наук и использования их в отраслях, связанных с обеспечением безопасности Российской Федерации, в интересах здравоохранения, обеспечения обороны государства, защиты окружающей среды.

1.2. Для осуществления научной и научно-технической деятельности на предприятии используются следующие информационные активы:

– информационные ресурсы, содержащие персональные данные (ПДн) регистрантов и работников ФГУП ЮУрИБФ;

– информационные ресурсы, содержащие сведения, составляющие коммерческую, государственную тайну, сведения ограниченного распространения, а также открыто распространяемая информация;

– информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и хранения, а также системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

1.3. Действие настоящей Политики не распространяется на устанавливаемый государственными органами режим защиты сведений, составляющих государственную тайну Российской Федерации.

1.4. Информационная безопасность (ИБ) – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке. Конфиденциальность – свойство, заключающееся в недоступности информации или не раскрытии ее содержания для неавторизированных лиц, субъектов или процессов. Целостность – свойство, заключающееся в обеспечении точности и полноты ресурсов. Доступность – свойство, заключающееся в доступности и применимости для авторизованных субъектов, когда потребуется.

1.5. Целью обеспечения информационной безопасности является соблюдение конфиденциальности, целостности и доступности информации.

1.6. Информационная безопасность является одним из основных инструментов, обеспечивающих возможность совместного использования информации.

1.7. Целью системы управления информационной безопасностью (СУИБ) является создание, внедрение, эксплуатация, мониторинг, анализ, сопровождение и совершенствование ИБ.

1.8. СУИБ является неотъемлемой частью общей системы управления предприятием.

1.9. Руководство ФГУП ЮУрИБФ осознает важность и необходимость ИБ, создания, внедрения, развития и совершенствования СУИБ, мер и средств обеспечения ИБ. Требования ИБ соответствуют интересам (целям) деятельности предприятия и предназначены для снижения рисков, связанных с ИБ, до приемлемого уровня.

2. Принципы деятельности по отношению к ИБ и СУИБ

2.1. Настоящая Политика является документом первого уровня по ИБ и СУИБ и устанавливает общее направление и принципы деятельности по отношению к ИБ.

2.2. Принцип законности: соблюдение норм международного права, Конституции Российской Федерации и законодательства Российской Федерации при осуществлении деятельности по обеспечению информационной безопасности.

2.3. Принцип сбалансированности: соблюдение баланса интересов субъектов и общества, их взаимная ответственность.

2.4. Принцип системности и комплексности. СУИБ должна использовать комплекс нормативных, экономических, технических, программных и организационных мер. В СУИБ должна быть обеспечена непрерывность функционирования ИБ на всех жизненных циклах системы. На постоянной основе должен проводится мониторинг и аудит эффективности системы и своевременная ее модернизация.

2.5. Принцип открытости: информирование работников организации, субъектов персональных данных о деятельности предприятия в области ИБ.

2.6. Принцип реальности выдвигаемых задач и экономической эффективности с учетом имеющихся ресурсов, сил и средств.

2.7. Принцип сочетания централизованного управления силами и средствами обеспечения безопасности с передачей части полномочий в этой области руководителям и ответственным работникам структурных подразделений.

3. Организация ИБ

3.1. В целях организации ИБ на предприятии создается организационная инфраструктура ИБ.

3.2. Административная структура СУИБ ФГУП ЮУрИБФ состоит из:

- директора;
- ответственного за обработку ПДн;
- руководителя группы по организации и обеспечению ИБ (группа ИБ);
- руководителя группы компьютерных технологий;
- руководителей подразделений, сотрудникам которых предоставлен доступ к ПДн;
- лица, ответственных за ИБ в подразделениях;
- ответственный за обеспечение физической безопасности.

3.3. Общее руководство организацией работ по обработке и обеспечению безопасности ПДн осуществляет Директор.

3.4. Ответственный за обработку ПДн организует обработку ПДн, с использованием и без использования средств автоматизации. Работа с ПДн организуется в соответствии с принципами деятельности по отношению к ИБ и СУИБ. Ответственный за обработку ПДн осуществляет контроль над соблюдением нормативных правовых актов, в том числе локальных по вопросам ИБ.

3.5. В целях соответствия принципам централизации управления, системности и комплексности подходов к СУИБ на предприятии создается группа ИБ.

3.6. Основными задачами группы ИБ являются:

- Создание СУИБ, в том числе установление подходов к оценке рисков, идентификация рисков, механизмов контроля для обработки рисков, механизмов предотвращения появления и обнаружения угроз;

– Внедрение и эксплуатация СУИБ, основанная на принципах системности и непрерывности;

– Мониторинг и анализ СУИБ, в том числе контроль доступа к ПДн;

– Сопровождение и совершенствование СУИБ.

4. Вопросы ИБ, связанные с персоналом

4.1. Нарушения, связанные с человеческим фактором, являются наиболее вероятными рисками для ИБ ФГУП ЮУрИБФ.

4.2. В рамках управления ИБ в трудовых договорах, должностных инструкциях, инструкции пользователя компьютерной информационной сетью, иными локальными нормативными правовыми документами четко определяются общие и конкретные обязанности работников, включая соглашения о конфиденциальности, меры реагирования на инциденты.

4.3. Важной составляющей СУИБ является обеспечение уверенности в осведомленности пользователей об угрозах и проблемах, связанных с ИБ, их оснащенности всем необходимым для соблюдения требований политики ИБ.

5. Заключительные положения

5.1. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в области обеспечения информационной безопасности, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, а также требованиями Федерального Агентства по техническому регулированию и метрологии.

5.2. Настоящая Политика является локальным нормативным актом ФГУП ЮУрИБФ.

5.3. Пересмотр Политики должен проводиться в соответствии с изменениями, влияющими на основу первоначальной оценки риска, в связи с изменениями организационной или технологической структуры, а также в связи с изменением законодательства в области информационной безопасности. Периодические пересмотры должны осуществляться на регулярной основе не реже одного раз в пять лет. Изменения вносятся в установленном на предприятии порядке. Ответственность за внесение изменений возлагается на руководителя группы по организации и обеспечению информационной безопасности.

5.4. Требования Политики обязательны для выполнения всеми работниками ФГУП ЮУрИБФ.

5.5. Лица, виновные в нарушении требований настоящей Политики, в том числе руководство предприятия, несут ответственность в пределах, определенных административным, уголовным и гражданским законодательством Российской Федерации.

Ведущий юрисконсульт С.Н. Габбасова

Ответственный за обработку ПДн М.Э. Сокольников

Руководитель группы ИБ П.В. Окатенко