Приложение к приказу № 22
об утверждении Положения
об информационной безопасности
от «02» октября 2023 года

ПОЛОЖЕНИЕ
об информационной безопасности в Фонде грантов
Главы Республики Карелия

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила защиты информации Фонда грантов Главы Республики Карелия (далее — Фонда, организации) определяют:

– процедуры обеспечения Фонда конфиденциальности информации о лицах, проектной документации, открытых банковских счетах некоммерческих организаций и иной информации, связанной с деятельностью Фонда и его взаимоотношениями с контрагентами.

– порядок доступа к вышеуказанной информации должностных лиц и сотрудников Фонда;

– правила предоставления вышеуказанной информации иным лицам.

1.2. Правила защиты информации Фонда разработаны в соответствии со следующими документами:

– Федеральный закон от 27.07.2006 N 149–ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 14.07.2022 N 266–ФЗ «О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности »;

– Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных»;

– Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 г. № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;

– Приказ Федеральной службы безопасности России от 13.02.2023 г. № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование

ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных»;

– ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Должностное лицо – для целей настоящих Положения руководитель Фонда.

2.2. Доступность информации – свойство информации, состоящее в том, что информация предоставляется авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

2.3. Информационная безопасность (ИБ) – защищенность Фонда от угроз в информационной сфере.

2.4. Инцидент ИБ – одно или серия связанных нежелательных или неожиданных Событий ИБ (в том числе компьютерных инцидентов), которые могут привести к риску нарушения выполнения бизнес–процессов, технологических процессов Фонда, повлечь иные негативные последствия.

2.5. Информация – информация о физических и юридических лицах, с которыми взаимодействует Фонд в рамках своей установленной Уставом организации деятельности.

2.6. Информационный ресурс – совокупность документов, содержащих Информацию, структурированных в базы данных Фонда на цифровых и физических носителях.

2.7. Информационная система – совокупность Информационных ресурсов, Информационных технологий и технических средств.

2.8. Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения Информации и способы осуществления таких процессов и методов.

2.9. Конфиденциальность информации – свойство информации, состоящее в том, что обработка, хранение и ее передача осуществляется таким образом, что эта информация доступна только авторизованным пользователям, объектам информационной системы или процессам.

2.10. Обслуживающий персонал – обслуживающий персонал, имеющий доступ во внутренние помещения Фонд, где могут находиться документы и материальные носители, содержащие Информацию, а также к техническим средствам и программному обеспечению используемым для обработки Информации, для целей технического и административного обслуживания здания, технических средств, позволяющих осуществлять обработку Информации, в том числе Работники Фонда и лица, исполняющие обязательства по заключенным с Фондом договорам.

2.11. Органы управления Фондом – высший коллегиальный орган Фонда (Наблюдательный совет) и единоличный исполнительный орган (Генеральный директор).

2.12. Пользователь – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации.

2.13. Работник – физическое лицо, выполняющее в Фонде работу по трудовому договору (контракту) или оказывающее услуги (выполняющее работы) для организации на основании гражданско–правового договора.

2.14. Событие информационной безопасности (событие ИБ) – идентифицированное возникновение и (или) изменение состояния объектов информатизации финансовой организации, действия работников финансовой организации и (или) иных лиц, указывающие на возможный (потенциальный) инцидент защиты информации.

2.15. Система обеспечения информационной безопасности (СОИБ) – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение и систему управления Фонда, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки СОИБ.

2.16. Третьи лица – лица, не относящиеся к Пользователям и Обслуживающему персоналу.

2.17. Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

III. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Защита Информации осуществляется путем построения комплексной СОИБ, реализующей меры по защите Информации.

3.2. Целью СОИБ является обеспечение устойчивого и эффективного функционирования Фонда и защита его клиентов и других контрагентов от угроз в информационной сфере.

3.3. Основные принципы СОИБ:

–одним из наиболее ценных активов Фонда является создаваемая, обрабатываемая и используемая Информация, в том числе переданная и получаемая от Фонда ее клиентам;

– обеспечение Фонда конфиденциальности, целостности и доступности Информации;

– обеспечение Фонда бесперебойной доступности услуг и сервисов организации в сроки, определенные законодательством, договорами с клиентами, внутренними регламентами Фонда и иными документами;

– непрерывность функционирования мер защиты Информационных систем;

– требования настоящего Положения должны быть реализованы на всех уровнях информационной инфраструктуры – во всех системах, внутренних и внешних процессах функционирования организации.

3.4. Требования СОИБ распространяются на:

– Пользователей и Обслуживающий персонал, включая всех Работников и Должностных лиц, взаимодействующих с Информацией Фонда;

– здания и помещения, в которых осуществляет свою деятельность Фонд (Республика Карелия, г.Петрозаводск, ул.Германа Титова, д. 3, помещ. 1);

– процессы, в том числе организованные в дистанционном формате.

3.5. Для исполнения поставленной цели, СОИБ реализует следующие задачи:

– разработка и применение защитных мер на всех этапах обработки Информации;

– реализация системы своевременного обнаружения Инцидентов ИБ;

– контроль выбранных защитных мер в области ИБ;

– постоянное совершенствования СОИБ, которое включает анализ собственного опыта и опыта других организаций, в том числе международных и использование результатов такого анализа.

3.6. Информация о инцидентах ИБ, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных осуществляется через Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

IV. МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Для защиты Информации СОИБ внедрены в том числе следующие меры:

–реализация разрешительной системы доступа (включая разграничение доступа цифровой информации и информации, находящейся на физических носителях);

– ограничение доступа в помещения;

– учет съемных носителей Информации, правила их хранения и обращения;

– внедрение средств защиты Информации;

– по предотвращению внедрения вредоносных программ и программных закладок;

– установление принципов взаимодействии с сетями связи общего пользования;

– внедрение и реализация правил передачи Информации Третьим лицам.

4.2. Система доступа включает в себя:

4.2.1. Доступ Пользователей (Обслуживающего персонала) к информационным ресурсам, информационным системам и связанным с их использованием работам, документам (далее – доступ) носит разрешительный характер и может быть

предоставлен только с личного устного или письменного распоряжения Генерального директора Фонда или лица его замещающего.

4.2.2. Запрет доступа реализуется с помощью физических и технических ограничений и может быть введен или снят письменным распоряжением Генерального директора Фонда или лица его замещающего.

4.2.3. Доступ производится на основании документированных и согласованных запросов и договоров.

4.2.4. Доступ Должностным лицам и Работникам предоставляется после заключения соглашения о неразглашении информации, которое может являться как самостоятельным документом, так и входить в состав обязательств работника или исполнителя по договору.

4.2.5. Доступ предоставляется в соответствии с функционалом каждого Работника и Должностного лица и предоставляется в объеме необходимом для исполнения ими своих обязанностей, который определяется в том числе с учетом того, являются ли они Пользователями или Обслуживающим персоналом при взаимодействии с Информацией.

4.2.6. Доступ осуществляется с использованием как средств парольной защиты, так и с помощью дополнительных факторов аутентификации.

4.2.7. Осуществляется разграничение доступа Пользователей и Обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации. Разграничение доступа реализуется посредством использования ролевой модели доступа с выполнением принципа минимальной достаточности.

4.2.8. Объем доступа контролируется и пересматривается на периодической основе, и прекращается при выявлении отсутствия необходимости в доступе, в том числе при увольнении Должностных лиц и Работников.

4.3. Доступ в помещения включает в себя:

4.3.1. Доступ Пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку Информации, связанной с деятельностью Фонд, а также хранятся носители такой Информации ограничен.

4.3.2. Вышеуказанные помещения оборудованы системой контроля и управления доступом.

4.3.3. Доступ предоставляется Работникам и Должностным лицам только в помещения, доступ в которые необходим таким лицам непосредственно для выполнения ими своих должностных обязанностей.

4.4. В Фонде предусмотрены следующие процедуры по регистрации действий Пользователей и Обслуживающего персонала и контролю несанкционированных доступа и действий Пользователей, Обслуживающего персонала и посторонних лиц:

4.4.1. События ИБ контролируются на предмет несанкционированного доступа и действий пользователей.

4.4.2. Факты изменения настроек и активации новых Пользователей в Информационных системах проверяются на легитимность.

4.4.3. Факты несанкционированных действий анализируются с целью выработки мер по предотвращению реализации угроз.

4.5. В Фонде действуют следующие процедуры по учету и хранению съемных носителей информации и их обращению, целью которых является исключение хищения, подмены и уничтожения Информации:

4.5.1. Осуществляется учет и контроль использования съемных носителей, содержащих Информацию.

4.5.2. Использование неучтенных носителей запрещено.

4.5.3. Съемные носители при каждом подключении к компьютерной технике (использовании) проходят контроль на наличие вредоносных программ.

4.5.4. Хранение съемных носителей осуществляется в местах, доступ в которые ограничен.

4.5.5. Возврат съемных носителей осуществляется в обязательном порядке при увольнении Работника и Должностного лица.

4.6. В Фонде функционируют следующие средства защиты Информации**:**

– средства идентификации и аутентификации;

– средства разграничения доступа;

– парольная защита;

– средства защиты от вредоносных программ и спама;

– специализированные программные средства анализа по выявлению вредоносного ПО и уязвимостей в настройках операционной системы (сканер уязвимостей).

4.7. С целью предотвращения внедрения в Информационные системы вредоносных программ (программ– вирусов) и программных закладок в Фонд реализуются следующие меры защиты:

4.7.1. На всех серверах и рабочих станциях установлены антивирусные средства защиты с регулярно обновляемыми базами вирусов.

4.7.2. Осуществляется периодическое сканирование элементов Информационных систем на наличие вредоносных программ и программных закладок.

4.7.3. Применяется только лицензионное программное обеспечение или программное обеспечение, разработанное по заказу Фонда и прошедшее соответствующее тестирование.

4.7.4. Соглашениями на предоставление программного обеспечения/права на использования программного обеспечения предусмотрена ответственность лицензиара/разработчика программного обеспечения за наличие программных закладок в программном обеспечении.

4.7.5. Все подключаемые к компьютерам носители Информации проверяются на наличие вредоносных программ.

4.7.6. На серверах электронной почты применяются средства защиты от спама.

4.8. При взаимодействии Информационных систем Фонда с информационно–телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) не применяются дополнительные меры защиты Информации.

4.9.1. Фонд обеспечивает конфиденциальность Информации. Доступ к Информации Третьим лицам предоставляется только в случаях и объеме, установленных законодательством РФ и договорами с Депонентами.

V. ФУНКЦИИ И ОБЯЗАННОСТИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. В рамках деятельности по обеспечению ИБ указанные ниже Органы управления, Должностные лица, Работники, Пользователи и Обслуживающий персонал выполняют следующие функции и имеют следующие обязанности:

5.2. Наблюдательный Совет:

– получение информации о статусе и контроль СОИБ;

– оценка вреда, который может быть причинен Пользователям, Работникам и Обслуживающему персоналу в случае нарушения Федерального закона от 27.07. 2006 года N 152-ФЗ «О персональных данных».

5.3. Должностные лица:

– соблюдение Правил и контроль их соблюдения Работниками, входящими в их структурных подразделениях;

– информирование НКЦКИ об инцидентах ИБ.

5.4. Работники:

– соблюдение требований законодательных и нормативных документов, в том числе внутренних нормативных документов Фонда по вопросам информационной безопасности.

5.5. Пользователи и Обслуживающий персонал (если не являются Работниками и Должностными лицами Фонда и при этом им предоставлен доступ к Информации):

– соблюдение требований информационной безопасности, устанавливаемых законодательными и нормативными документами, нормативными документами Фонда, а также договорами и соглашениями, стороной которых является Фонд.

5.6. Неисполнение Работниками, Должностными лицами а также Пользователями и Обслуживающим персоналом обязанностей по обеспечению ИБ является основанием для отключения доступа к Информационным системам и Информации, а также применения мер воздействия, в соответствии с внутренними документами Фонд и требованиями законодательства РФ.

VI. ПЕРЕСМОТР И АКТУАЛИЗАЦИЯ ПОЛОЖЕНИЯ

6.1.Настоящее Положение пересматривается и актуализируется приказом Генерального директора при изменении законодательства и нормативно–правовых актов Российской Федерации, нормативных актов и требований регулирующих органов, а также при изменениях в процессах функционирования Фонда, требующих внесение изменений в Положение.