

Приложение
к приказу Российского фонда
развития информационных технологий
от 24. 01. 2025 г. № 1

ПОЛОЖЕНИЕ
о порядке обращения с конфиденциальной информацией
в Российском фонде развития информационных технологий

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о порядке обращения с конфиденциальной информацией в Российском фонде развития информационных технологий (далее – Положение) является локальным актом Российского фонда развития информационных технологий (далее – Фонд), регулирующим процесс обращения с конфиденциальной информацией в Фонде.

1.2. Положение является обязательным для исполнения всеми работниками Фонда.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Владельцы конфиденциальной информации РФРИТ – штатные работники Фонда с полной или частичной занятостью, самостоятельно создавшие конфиденциальную информацию, имеющее право разрешать, и ограничивать доступ к информации.

Доступ к конфиденциальной информации – ознакомление определенных лиц с конфиденциальной информацией с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Защита конфиденциальной информации – действия по принятию правовых, организационных и технических мер, направленных на:

а) обеспечение защиты информации от неправомерного доступа, обработки, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий, включая утечку, в отношении такой информации;

б) соблюдение конфиденциальности информации.

Конфиденциальная информация – информация (включая рабочие материалы, документы, сведения, переписку, данные), имеющая действительную или потенциальную производственную, организационную, коммерческую, научно-технологическую, финансово-экономическую и иную ценность в силу ее неизвестности третьим лицам, доступ к которой в том числе ограничен локальными актами Фонда, договорами (соглашениями) с контрагентами Фонда, а также иными документами в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к конфиденциальной информации, требование не допускать утечку такой информации третьим лицам без согласия её владельца.

Фонд – Российский фонд развития информационных технологий.

Нарушение режима защиты конфиденциальной информации – умышленные или непреднамеренные действия, или бездействие работников Фонда (умышленные действия третьих лиц), приведшие к утечке конфиденциальной информации, либо к утрате (включая разглашение или уничтожение) документов (как бумажных, так и электронных), содержащих такую информацию.

Обработка конфиденциальной информации – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с конфиденциальной информацией (в т.ч. персональными данными), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение данных.

Обладатель конфиденциальной информации – лицо, получившее конфиденциальную информацию установленным порядком.

Общедоступная информация – не относящаяся к конфиденциальной информация, разглашение которой не оказывает негативного влияния на деятельность Фонда, не подлежит защите и официально разрешенная к опубликованию в соответствии с локальными актами Фонда.

Пользователь конфиденциальной информации – работник Фонда, получивший доступ к конфиденциальной информации в целях выполнения должностных обязанностей.

Предоставление конфиденциальной информации – действия, направленные на получение конфиденциальной информации определенным кругом лиц или передачу информации определенному кругу лиц.

Разглашение конфиденциальной информации – действие или бездействие, в результате которых нарушается защита конфиденциальной информации в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств), информация становится известной неуполномоченным работникам Фонда или третьим лицам без согласия владельца информации, с нарушением правил обращения с конфиденциальной информацией, установленных в Фонде, либо договорами (соглашениями) с контрагентами и грантополучателями.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Работники (работники Фонда) – штатные работники Фонда с полной или частичной занятостью, независимо от их должности в Фонде.

Режим защиты – установленная процедура доступа к соответствующим сведениям и ответственность за разглашение этих сведений.

Утечка конфиденциальной информации – событие, при котором в нарушение требований Положения, конфиденциальная информация становится

доступной третьим лицам или работникам Фонда как в результате вмешательства третьих лиц, так и в результате действий (или бездействий) работников Фонда.

Электронный документ – информация, представленная в электронной (цифровой) форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин или иных электронных считывателей информации, а также для передачи по информационно-телекоммуникационным и компьютерным сетям или обработки в информационных системах.

3. ОСНОВНЫЕ ПОЛОЖЕНИЯ

3.1. Положение устанавливает общие требования к организации обращения и защиты конфиденциальной информации в подразделениях Фонда.

3.2. Руководители структурных подразделений Фонда несут персональную ответственность за организацию и обеспечение режима защиты при организации работы подчиненных им структурных подразделений, контролируют выполнение установленных Положением режимных требований, обеспечивают ограничение возможности ознакомления с информацией работников, которым по роду выполняемых должностных обязанностей конфиденциальная информация не требуется.

3.3. Все работники Фонда обязаны знать, какие сведения относятся к конфиденциальной информации Фонда.

4. ПОРЯДОК И ПРАВИЛА КАТЕГОРИРОВАНИЯ ИНФОРМАЦИИ

4.1. Информация, обращающаяся в Фонде, подразделяется на два типа:

- общедоступную информацию (приложение № 1 к Положению);
- конфиденциальную информацию – информацию, доступ к которой ограничен (приложение № 2 к Положению).

4.2. В отдельных случаях, по решению Заместителя генерального директора, курирующего вопросы безопасности или директора департамента экспертизы и безопасности РФРИТ, на исходящих и/или внутренних документах Фонда, относящихся к категории конфиденциальной информации, может быть проставлен специальный гриф:

КОНФИДЕНЦИАЛЬНО
РОССИЙСКИЙ ФОНД РАЗВИТИЯ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
123242, Москва, Новинский бульвар, д. 31, 5 этаж

4.3. Документы на бумажном носителе с грифом, указанным в пункте 4.2, подлежат регистрации с указанием количества экземпляров и хранятся в специальном(ых) деле(ах) в порядке, определенном заместителем генерального директора, курирующего вопросы безопасности, директором департамента экспертизы и безопасности РФРИТ.

5. ДОПУСК К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В целях защиты конфиденциальной информации, обрабатываемой при осуществлении уставной деятельности, определяется следующее:

5.1. Лица, принятые на работу в рамках трудового договора или на основании гражданско-правового договора, принимают на себя обязательство не разглашать конфиденциальную информацию.

5.2. При оформлении трудовых отношений между Фондом и работником, работник подписывает обязательство о неразглашении конфиденциальной информации по форме согласно приложению № 3 к Положению.

5.3. Работники Фонда должны запрашивать и получать доступ к конфиденциальной информации только в пределах и объеме, необходимом для выполнения ими своих должностных обязанностей.

5.4. Генеральный директор, заместитель генерального директора, курирующий вопросы безопасности, директор департамента экспертизы и безопасности имеют неограниченное право доступа ко всем документам на материальных или электронных носителях, содержащим конфиденциальную информацию.

5.5. Заместители генерального директора Фонда, руководители структурных подразделений Фонда, иные работники, подписавшие обязательство о неразглашении конфиденциальной информации согласно приложению № 3 к Положению по согласованию с генеральным директором или владельцами конфиденциальной информации, могут иметь доступ к конфиденциальной информации, относящийся к их должностным обязанностям.

5.6. Основаниями для прекращения доступа к конфиденциальной информации являются:

- приказ об увольнении работника, соглашение о расторжении трудового договора (гражданско-правового договора);
- заявление работника об увольнении либо уведомление работнику в соответствии с трудовым законодательством Российской Федерации о предстоящем увольнении;
- нарушение работником взятых на себя обязательств, связанных с неразглашением конфиденциальной информации;
- решение генерального директора Фонда об отстранении работника от работы с конфиденциальной информацией.

6. ПОРЯДОК ОБРАЩЕНИЯ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

6.1. Владельцы конфиденциальной информации, а также работники Фонда, получившие доступ к конфиденциальной информации обязаны обеспечить сохранность ставшей им известной информации и не допускать ее утечку (включая несанкционированное раскрытие третьим лицам).

6.2. Решение о предоставлении доступа к конфиденциальной информации принимается руководителем структурного подразделения работника, создавшего конфиденциальную информацию, курирующим заместителем генерального

директора или генеральным директором.

6.3 Передача конфиденциальной информации может осуществляться по каналам корпоративной электронной почты («логин»@rfrit.ru) и другим корпоративным информационным системам. Передача конфиденциальной информации с помощью мессенджеров, некорпоративных облачных хранилищ и съёмных носителей запрещена.

При передаче конфиденциальной информации по корпоративной электронной почте и другим корпоративным информационным системам, в зависимости от категории, необходимо использовать следующий текст, который в обязательном порядке должен быть включен в подпись работника:

«Настоящее сообщение содержит охраняемую законом конфиденциальную информацию, относящуюся к категории «конфиденциально» и предназначено только для указанных в письме получателей. Содержание данного сообщения не должно быть раскрыто или использовано любым лицом, кроме получателей. Если данное сообщение попало к Вам по ошибке, пожалуйста, незамедлительно уведомите об этом отправителя, а само сообщение уничтожьте».

Печать документов категории «конфиденциально» может осуществляться на принтере только в зоне визуального контроля с немедленным изъятием копий.

6.4. Конфиденциальная информация может быть передана другим уполномоченным работникам Фонда владельцем конфиденциальной информации по предварительному согласованию с руководителем структурного подразделения работника, создавшего конфиденциальную информацию, либо курирующим заместителем генерального директора или генеральным директором. Остальные работники Фонда, получившие доступ к конфиденциальной информации, не имеют права самостоятельно передавать ставшую им известной конфиденциальную информацию, если они не являются ее владельцами и, если они не получили разрешение от руководителя структурного подразделения работника, создавшего конфиденциальную информацию, курирующего заместителя генерального директора указанного подразделения или генерального директора.

6.5. При передаче конфиденциальной информации третьим лицам необходимо использовать специализированную программу CryptFL согласно приложению № 4 к Положению. Перед передачей необходимо убедиться, что с третьими лицами заключен договор о неразглашении конфиденциальной информации (приложение № 5).

6.6. Поступившая на бумажном носителе входящая корреспонденция, указанная в пункте 4 Приложения № 2 к Положению, подлежащая официальной регистрации в установленном порядке, должна быть передана внутри Фонда уполномоченным работникам на бумажном носителе с обязательным внесением соответствующей записи в реестр передачи информации ограниченного доступа по форме согласно приложению № 6 к Положению.

7. ОБЯЗАННОСТИ РАБОТНИКОВ, ДОПУЩЕННЫХ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

7.1. Заместители генерального директора Фонда, советники генерального директора, руководители структурных подразделений, а также лица их замещающие несут ответственность за организацию режима защиты конфиденциальной информации в подчиненных им структурных подразделениях в соответствии с Положением.

7.2. Руководители структурных подразделений, руководствуясь Положением, требованиями законодательства Российской Федерации по защите конфиденциальной информации, обеспечивают обращение конфиденциальной информации, обрабатываемой в структурном подразделении, внутри Фонда и при предоставлении третьим лицам.

7.3. Работники Фонда обязаны знать, какая информация подлежит защите и принимать все необходимые меры по защите конфиденциальной информации, не разглашать ее, в том числе и среди работников Фонда, соблюдать установленный порядок работы с третьими лицами, соблюдать порядок обращения с конфиденциальной информацией, не допускать утечку конфиденциальной информации, соблюдать правила делопроизводства.

7.4. Работники Фонда не имеют права использовать конфиденциальную информацию в личных целях, а также заниматься прямо или косвенно какой-либо деятельностью, связанной с использованием конфиденциальной информации Фонда в ущерб Фонду.

7.5. Работники Фонда имеют право знакомиться только с той конфиденциальной информацией, которая необходима им для выполнения должностных обязанностей.

7.6. Работники Фонда обязаны:

7.6.1. В случае непреднамеренного доступа к конфиденциальной информации (например, документированная информация оставлена на принтерах, либо в местах общего доступа), обнаружения нарушения порядка учета, хранения и использования конфиденциальной информации передать данную информацию своему руководителю, заместителю генерального директора, курирующего вопросы безопасности или директору департамента экспертизы и безопасности;

7.6.2. Выполнять требования к обращению с конфиденциальной информацией, предусмотренные Положением и другими локальными актами Фонда, регламентирующими вопросы обеспечения режима защиты и порядка обращения с конфиденциальной информацией;

7.6.3. Не разглашать конфиденциальную информацию, полученную в результате выполнения своих должностных обязанностей и предпринимать все возможные меры в рамках своих полномочий для недопущения утечки конфиденциальной информации;

7.6.4. Соблюдать установленные в Фонде правила работы с документами, порядок их учета, хранения и уничтожения;

7.6.5. Знакомиться только с теми документами и информацией, к которым получили допуск в силу своих должностных обязанностей;

7.6.6. Во время работы с конфиденциальной информацией принимать меры к исключению возможности ознакомления с ними других лиц;

7.6.7. Оповещать директора департамента экспертизы и безопасности о действиях других лиц, способных привести к разглашению конфиденциальной информации или ее утечки;

7.6.8. При составлении документов на бумажном носителе, содержащих конфиденциальной информации ограничиваться минимальной, действительно необходимой конфиденциальной информацией;

7.6.9. Определять количество экземпляров документа на бумажном носителе в строгом соответствии с необходимостью;

7.6.10. Документы на бумажном носителе, содержащие конфиденциальную информацию хранить отдельно от документов с общедоступной информации;

7.6.11. В нерабочее время, а также при кратковременном отсутствии на рабочем месте документы, содержащие конфиденциальную информацию, в том числе на электронных носителях, хранить в местах, исключающих доступ посторонних лиц;

7.6.12. Незамедлительно информировать руководителя структурного подразделения, заместителя генерального директора, осуществляющего контроль и координацию деятельности структурного подразделения и директора департамента экспертизы и безопасности о фактах утраты (недостачи) документов (отдельных листов/файлов) и электронных носителей, содержащих конфиденциальную информацию, ключей от шкафов (сейфов), фактах обнаружения неучтенных документов с конфиденциальной информацией, а также о фактах необоснованного интереса к конфиденциальной информации, со стороны лиц, не имеющих прямого отношения к работе с конфиденциальной информацией;

7.6.13. При увольнении, переводе на другую работу (должность), убытии в отпуск, длительную командировку (более 1 месяца) передать документы, содержащие конфиденциальную информацию, руководителю структурного подразделения (лицу его замещающему), исключить доступ посторонних лиц на время отсутствия к документам, содержащим конфиденциальную информацию;

7.6.14. Соблюдать правила разграничения доступа к конфиденциальной информации, неукоснительно выполнять требования локальных актов Фонда по организации доступа к информационным ресурсам, организации парольной и антивирусной защиты;

7.6.15 Не разглашать свои индивидуальные пароли на доступ к компьютерным, сетевым и иным информационным ресурсам, на которых хранится конфиденциальная информация. Не использовать чужие пароли. Выполнять требования соответствующих администраторов вычислительной сети и администраторов автоматизированных (информационных) систем по смене паролей, не применять простых паролей;

7.6.16. Принимать меры к исключению ознакомления посторонних лиц с конфиденциальной информацией, выводимой на экран дисплея;

7.6.17. Не использовать (не загружать, не запускать и т.п.) для обработки конфиденциальной информацией сторонние программные средства, не допущенные для применения в Фонде. При требовании операционной системы

обновления установленного программного обеспечения обязательно известить заместителя директора департамента экспертизы и безопасности и не осуществлять обновление без их разрешения;

7.6.18. При необходимости покинуть свое рабочее место провести стандартные процедуры выхода из системы и отключения компьютера. В рабочее время допускается блокировка доступа к компьютеру с использованием аппаратно-программных средств при работе с конфиденциальной информацией;

7.6.19. Не допускать случаев передачи конфиденциальной информации через сеть Интернет и иные публичные сети (включая факс), не отправлять конфиденциальную информацию по не корпоративной электронной почте, не передавать с использованием некорпоративных облачных хранилищ. Не фотографировать, не обсуждать конфиденциальную информацию в присутствии третьих лиц;

7.6.20. Не допускать применения средств криптографической защиты и защиты от несанкционированного доступа, не принятых в эксплуатацию в Фонде или не предусмотренных эксплуатационной (технической) документацией на информационные и автоматизированные системы;

7.6.21. В нерабочее время, а также при кратковременном отсутствии на рабочем месте хранить съемные электронные (и иные) носители, содержащие конфиденциальную информацию в местах, исключающих доступ посторонних лиц;

7.6.22. Немедленно информировать руководителя структурного подразделения и заместителя директора экспертизы и безопасности о фактах или возможности несанкционированного доступа к информации в локальной вычислительной сети (ЛВС) Фонда;

7.6.23. Не допускать хранение документов, содержащих конфиденциальную информацию, на рабочих столах. Каждый работник Фонда несет персональную ответственность (дисциплинарную, административную и уголовную) за оставление в открытом доступе документов, содержащих конфиденциальную информацию. Работники Фонда должны строго соблюдать следующие правила:

- работник должен защищать конфиденциальную информацию от разглашения и утечки;
- конфиденциальная информация не должна быть доступна третьим лицам;
- все электронные носители информации (usb, карты памяти, CD-диски и др.) не должны оставаться в открытом доступе;
- компьютеры и ноутбуки должны быть заблокированы в отсутствии работника;
- запрещено оставлять распечатанные документы на/в принтере;
- после завершения работы (рабочего дня) каждый работник Фонда должен убрать документы, содержащие конфиденциальную информацию, и электронные носители в места, исключающие доступ посторонних лиц;
- на доске для рисования или флип-чарте информация должна быть стерта или уничтожена по завершении рабочих встреч.

7.7. Работникам, допущенным к конфиденциальной информации, запрещается:

7.7.1. Снимать и изготавливать копии документов с конфиденциальной информацией (в том числе с электронных документов), делать из них выписки без разрешения руководителя структурного подразделения, либо работника, создавшего конфиденциальную информацию, либо курирующего заместителя генерального директора или генерального директора Фонда;

7.7.2. Выносить за пределы помещений Фонда документы и электронные (и иные) носители с конфиденциальной информацией без письменного разрешения руководителя структурного подразделения работника, создавшего конфиденциальную информацию, курирующего заместителя генерального директора или генерального директора;

7.7.3. Обсуждать вопросы, содержащие конфиденциальную информацию в присутствии посторонних лиц;

7.7.4. Сообщать устно или письменно посторонним лицам конфиденциальную информацию.

7.8. Работникам Фонда запрещается:

7.8.1. Подключать (или допускать подключение) к сети Фонда не корпоративные компьютеры и другие устройства;

7.8.2. Использовать для сохранения конфиденциальной информации личные (не принадлежащие Фонду) компьютеры (в том числе мобильные - ноутбуки, карманные персональные компьютеры (КПК), электронные записные книжки, смартфоны, мобильные телефоны и другие мобильные цифровые (вычислительные) устройства);

7.8.3. Использовать средства рабочей электронной почты для отправки нерабочей корреспонденции, сообщать персональные электронные почтовые адреса для получения нерабочей корреспонденции (в том числе электронных рассылок) через сеть Интернет.

7.8.4. Использовать мессенджеры, некорпоративные облачные хранилища и съемные носители для передачи конфиденциальной информации.

8. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ СТОРОННИМ ЛИЦАМ

8.1. Предоставление информации о деятельности Фонда органам государственной власти, иным государственным органам, органам местного самоуправления осуществляется в порядке, установленном законодательством Российской Федерации на основании мотивированного запроса, подписанного уполномоченным лицом. Конфиденциальная информация может предоставляться по мотивированному требованию органа государственной или муниципальной власти и управления, судебного органа. Мотивированное требование должно быть подписано уполномоченным должностным лицом и содержать указание цели и правового основания затребования конфиденциальной информации и срок предоставления этой информации, если иное не установлено законодательством Российской Федерации.

8.2. До момента начала обсуждения с третьими лицами документов с конфиденциальной информацией или их передачи, в обязательном порядке

заключается договор о неразглашении конфиденциальной информации. Либо договоры, заключаемые Фондом с третьими лицами, должны в обязательном порядке содержать раздел о конфиденциальной информации.

8.3. Передача конфиденциальной информации третьим лицам осуществляется при условии выполнения всех следующих условий:

- другая сторона уведомлена о том, что такая информация является конфиденциальной информацией;
- заключен договор, в котором имеется раздел о конфиденциальности (либо заключен договор о неразглашении конфиденциальной информации, либо соглашение о конфиденциальности) и включены, при необходимости, другие требования по обеспечению безопасности;
- соблюдены требования (правовые, организационные и технические) к защите, обрабатываемой конфиденциальной информации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении конфиденциальной информации;
- в обязанности лица, осуществляющего работу с конфиденциальной информацией, входит соблюдение защиты конфиденциальной информации и обеспечение безопасности информации при ее обработке;
- прописана ответственность за невыполнение определенных в договоре требований к защите конфиденциальной информации.

8.4. Действия с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение осуществляются в соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных», локальных актов Фонда.

9. ОПУБЛИКОВАНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

9.1. Запрещается публикация материалов, содержащих конфиденциальную информацию, в средствах массовой информации, включая Интернет и другие публичные сети, а также использование их в публичных выступлениях до снятия в установленном порядке существующих ограничений.

9.2. Возможность открытого оглашения (публикации) конфиденциальной информации, обладателем которой является Фонд, определяется генеральным директором Фонда.

9.3. Открытое оглашение (публикация) конфиденциальной информации, в отношении которой Фонд не является обладателем (собственником), может осуществляться при наличии письменного согласия обладателя (собственника) этой информации на ее открытое оглашение (публикацию), а также в иных случаях, предусмотренных законодательством Российской Федерации.

9.4. Работники, обнаружившие факт публикации в средствах массовой информации, включая Интернет, а также использования в публичных

выступлениях конфиденциальной информации, обязаны сообщить об этом генеральному директору Фонда, заместителю генерального директора, курирующему вопросы безопасности (или директору департамента экспертизы и безопасности).

10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

10.1 Разглашение конфиденциальной информации Фонда, или утрата документов, содержащих конфиденциальную информацию, относится к числу грубых нарушений трудовых обязанностей.

10.2. За разглашение конфиденциальной информации Фонда и его контрагентов, утрату документов, содержащих конфиденциальную информацию, а также за иные нарушения режима защиты конфиденциальной информации виновные лица несут дисциплинарную, материальную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации и локальными актами Фонда.