УТВЕРЖДАЮ

Директор ИХБФМ СО РАН

чл.-кор. РАН, д. х. н.

Пыщный Д. В.

«09» января 2019 г.

ИНСТРУКЦИЯ

по обеспечению сохранности конфиденциальной информации в Федеральном государственном бюджетном учреждении науки Институт химической биологии и фундаментальной медицины Сибирского отделения Российской академии наук

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с требованиями законодательства Российской Федерации. Она предусматривает организационные и административные меры по защите конфиденциальной информации с целью предотвращения возможного экономического и иного ущерба Федеральному государственному бюджетному учреждению науки Институт химической биологии и фундаментальной медицины Сибирского отделения Российской академии наук (далее — ИХБФМ СО РАН, Институт) со стороны юридических и физических лиц, вызванного их неправомерными или неосторожными действиями путем присвоения или разглашения конфиденциальной информации.

1.2. Под конфиденциальной информацией понимается сведения, связанные с задачами, решаемыми Институтом в соответствии с учредительными документами, информация, связанная с управлением, финансами и другими сферами деятельности Института, разглашение (искажение, передача, утечка и т. д.) которой может нанести ущерб интересам Института. К сведениям, составляющим конфиденциальную информацию, относятся сведения, предусмотренные *Перечнем сведений, составляющих коммерческую тайну, Перечнем сведений, составляющих конфиденциальную информацию,* и *Перечнем приоритетных направлений деятельности Института, в отношении любой информации о которых вводится режим ограничения доступа.*

1.3. Разглашением конфиденциальной информации следует считать следующие действия сотрудника:

- доведение до сведения неуполномоченных лиц в устной, письменной, электронной или иной форме конфиденциальной информации. Указанный факт может наступить в результате умысла сотрудника или по неосторожности, включая халатное отношение к своим обязанностям;
- использование конфиденциальной информации в процессе выполнения работы для другого предприятия, учреждения и организации или по заданию физического лица, иного субъекта предпринимательской деятельности без образования юридического лица;
- использование конфиденциальной информации в научной и педагогической деятельности;
- использование конфиденциальной информации в личных целях, не связанных с выполнением должностных обязанностей в Институте;
- использование конфиденциальной информации в ходе публичных выступлений, интервью и т. п. мероприятий;
- иные действия сотрудника, в результате которых конфиденциальная информация стала известна неуполномоченным ее получать лицам.

1.4. Не считаются разглашением конфиденциальной информации действия сотрудника, указанные в п. 1.3. настоящей Инструкции, совершенные им в порядке и в случаях, предусмотренных законодательством Российской Федерации, во исполнение нормативных актов Института или договоров (соглашений) Института с иными организациями или физическими лицами. Не считаются разглашением конфиденциальной информации действия сотрудника, совершенные им при наличии письменного разрешения или иного письменного указания руководства Института.

1.5. Предоставление конфиденциальной информации представителям контрольных, ревизионных, фискальных и следственных органов, депутатам Государственной Думы РФ, органам печати, радио, телевидения и т. п. допускается только с разрешения руководителя Института.

1.6. Защита конфиденциальной информации предусматривает:

- определение конфиденциальной информации и сроков ее защиты;
- систему допуска сотрудников Института, частных и командированных лиц к конфиденциальной информации;
- обязанности лиц, допущенных к конфиденциальной информации;
- порядок работы с бумажными документами, содержащими конфиденциальную информацию;
- порядок работы с электронными документами, содержащими конфиденциальную информацию;
- обеспечение сохранности документов и дел (архивов), содержащих конфиденциальную информацию;
- принципы организации и проведения контроля обеспечения установленного порядка при работе с конфиденциальной информацией;
- ответственность за разглашение конфиденциальной информации и утрату документов, содержащих конфиденциальную информацию.

1.7. Обязанности по конфиденциальному делопроизводству возлагаются на секретаря Директора (в части делопроизводства руководителя Института), Ученого секретаря Института (в части делопроизводства структурных подразделений) и системного администратора корпоративной компьютерной сети (в части обеспечения работоспособности электронной системы делопроизводства).

1.8. Конфиденциальная информация должна находиться преимущественно в электронном виде и быть защищена специальными криптографическими средствами.

1.9. Входящие конфиденциальные документы на бумажном носителе сотрудниками НОО переводятся в электронный вид, в дальнейшем работа с данными документами осуществляется сотрудниками в электронном виде.

1.10. Работа сотрудников с конфиденциальными документами на бумажном носителе допускается в виде исключения с разрешения руководства Института или руководства структурных подразделений в случае невозможности или нецелесообразности перевода документа в электронный вид.

1.11. После перевода конфиденциального входящего документа на бумажном носителе в электронный вид данный документ, по решению руководства Института или руководства структурного подразделения, уничтожается или, после отработки, определяется в соответствующее дело (архив).

1.12. Обмен конфиденциальными документами внутри организации осуществляется преимущественно в электронном виде с использованием средств электронной защиты.

1.13. Порядок работы с электронными конфиденциальными документами определен в части 2 данной Инструкции.

1.14. Определение вида исходящего конфиденциального документа (электронного или на бумажном носителе) возлагается на исполнителя по согласованию с руководством Института или руководством структурного подразделения.

1.15. Ответственность за ненадлежащие организацию работы с конфиденциальной информацией, разработку и осуществление необходимых мер по сохранности конфиденциальной информации руководитель Института возлагает на руководителей структурных подразделений, соответствующих должностных лиц Научно-организационного отдела, секретарей и системного администратора закрытой корпоративной компьютерной сети.

2. Порядок работы с конфиденциальной информацией, представленной в электронном виде

2.1. Хранение, работа и архивирование любых электронных конфиденциальных документов (файлов) должно осуществляться с учетом требования ограничения несанкционированного доступа к ним третьих лиц способами, оговоренными настоящим разделом данной Инструкции.

2.2. Все персональные компьютеры, установленные на рабочих местах сотрудников, подключены к защищенной корпоративной компьютерной сети Института (далее — Сеть).

2.3. Каждый персональный компьютер оснащен стандартным набором программных средств, принятых для эксплуатации в Институте. Любые изменения в оснащении персонального компьютера, подключенных к Сети, должны быть санкционированы руководством структурного подразделения, согласованы с администратором сети и осуществлены уполномоченными специалистами Института.

2.4. Вся конфиденциальная информация, имеющаяся в распоряжении сотрудника, должна храниться и обрабатываться на корпоративном файл-сервере Института.

2.5. Первичный допуск сотрудника к работе на персональном компьютере, включенного в Сеть, осуществляется системным администратором Сети по указанию руководства соответствующего структурного подразделения и включает в себя:

- ознакомление сотрудника с настоящей Инструкцией под роспись;
- инструктаж по порядку работы с программными средствами, принятыми для эксплуатации в Институте;
- получение сотрудником персонального ключа шифрования данных;
- получение сотрудником персонального пароля для доступа к ресурсам корпоративного сервера и локальной вычислительной сети;
- получение адреса персонального почтового ящика корпоративной почты.

2.6. Сотрудник, допущенный к работе с персональным компьютером, получает доступ:

- к персональному разделу на корпоративном файл-сервере («Личная» папка) для хранения и обработки электронных конфиденциальных документов (файлов), предоставленных в его распоряжение для выполнения поставленных перед ним задач;
- к разделу с открытыми ключами сотрудников Института;
- к персональному почтовому ящику корпоративной почты.

2.7. Все электронные конфиденциальные документы (файлы) должны храниться на корпоративном сервере одним из возможных способов:

- в личной папке сотрудника в защищенном личным ключом виде;
- в личной папке сотрудника в защищенном на личном плюс один или несколько открытых ключей уполномоченных сотрудников виде — в случае необходимости и по указанию руководства.

2.8. Все новые электронные конфиденциальные документы (файлы) должны создаваться только на файл-сервере в личной папке сотрудника.

2.9. Работа с электронными конфиденциальными документами (файлами) допускается только при условии расположения этих документов (файлов) на сервере способами, оговоренными п. 2.7.

2.10. В каждый конкретный момент времени в течение рабочего дня загруженными в персональный компьютер сотрудника должны быть только те электронные конфиденциальные документы (файлы), которые имеют непосредственное отношение к тому делу, которым занимается сотрудник в данный момент времени. При этом все другие конфиденциальные документы (файлы) должны находиться на сервере в виде, оговоренном п. 2.7.

2.11. Загрузка (открытие) сверх действительно необходимого количества электронных конфиденциальных документов (файлов) на персональных компьютерах сотрудников запрещается.

2.12. В течение рабочего дня ставшие ненужными в текущей работе (отработанные) электронные конфиденциальные документы (файлы) подлежат незамедлительному закрытию (сохранению на файл-сервер).

2.13. С целью предотвращения переполнения сетевых дисков, выявленные в течение дня ненужные файлы (старые версии файлов и т. д.) подлежат безусловному незамедлительному уничтожению.

2.14. Уничтожение электронных конфиденциальных документов (файлов) с сетевых дисков корпоративного файл-сервера осуществляется стандартными средствами операционной системы. Уничтожение электронных конфиденциальных документов (файлов) с любых иных носителей должно осуществляться только с помощью утилиты типа Wipe, специально предназначенной для уничтожения файлов без возможности их последующего восстановления.

2.15. Обмен электронными конфиденциальными документами (файлами) между сотрудниками, находящимися в Сети, осуществляется в зашифрованном виде с использованием сервиса корпоративной почты.

2.16. Обмен электронными конфиденциальными документами (файлами) между сотрудниками, находящимися вне Сети Института (командировки), осуществляется путем обмена зашифрованной почтой через корпоративные почтовые ящики сотрудников.

2.17. Порядок обращения с конфиденциальным бумажным документом, полученным в результате распечатки электронного конфиденциального документа, регламентируется соответствующими разделами данной Инструкции.

2.18. В случае прихода (ожидания) посетителя к сотруднику, в персональный компьютер этого сотрудника могут быть загружены только те конфиденциальные электронные документы (файлы), которые относятся к делу данного посетителя. Загружать в персональный компьютер и/или работать с электронными конфиденциальными документами (файлами), не относящимися к делу присутствующего посетителя, — запрещается.

2.19. Сотруднику, работающему с электронными конфиденциальными документами (файлами), категорически запрещается:

- оставлять персональный компьютер на время более пяти мин с разрешенным доступом к личной папке;
- сообщать кому бы то ни было свой персональный пароль доступа в закрытую корпоративную компьютерную Сеть Института;
- сообщать кому бы то ни было пароль доступа к своему персональному ключу шифрования;
- оставлять посетителя в кабинете без присмотра при включенном в защищенную корпоративную Сеть компьютере;
- хранить/обрабатывать личные файлы (данные, не имеющих отношения к выполнению функциональных обязанностей, а именно: файлы .mp3, игры, картинки, личные фотографии и т. п.) на сетевых дисках корпоративного сервера;
- использовать съемные носители — дискеты, ZIP-диски, магнитооптику и т. д. — для обмена между сотрудниками и хранения электронных конфиденциальных документов (файлов);
- самовольно, без согласования с администратором Сети, изменять аппаратную конфигурацию и настройки программного обеспечения персональных компьютеров, подключенных к Сети.

2.20. Сотрудник, работающий с электронными конфиденциальными документами (файлами), обязан:

- выполнять требования администратора Сети в рамках установленного регламента эксплуатации Сети и требований настоящей Инструкции (технический перерыв, устранение выявленных нарушений хранения/обработки данных, профилактические работы на оборудовании Сети). Несоблюдение требований настоящего пункта может привести к необратимой потере данных, ответственность за которую возлагается на самих сотрудников;
- при убытии в отпуск/командировку предоставить имеющиеся у него конфиденциальные электронные документы (файлы), которые могут понадобиться в его отсутствие (что определяется непосредственным руководителем), в распоряжение уполномоченного руководителем сотрудника в зашифрованном на открытом ключе этого сотрудника виде;
- ежедневно в конце рабочего дня производить «зачистку» локального диска своего персонального компьютера путем запуска соответствующей процедуры **нужно сделать эту процедуру**;
- еженедельно производить ревизию своей личной папки, размещенной на корпоративном файл-сервере, с целью выявления и уничтожения конфиденциальных электронных документов (файлов), ставших ненужными.

3. Определение конфиденциальной информации и обозначение документов на бумажном носителе, содержащих конфиденциальную информацию, и сроков ее защиты

3.1. На документах на бумажном носителе и делах (архивах), содержащих конфиденциальную информацию, проставляется гриф «Конфиденциально» или «Коммерческая тайна», а также номера экземпляров. Гриф и номера экземпляров проставляются в правом верхнем углу каждой страницы документа.

3.2. Необходимость проставления грифа «Конфиденциально» определяется исполнителем документа и утверждается руководством структурного подразделения, в соответствии с Перечнями, указанными в п. 1.2 настоящей Инструкции.

3.3. На наиболее важных конфиденциальных документах, с содержанием которых необходимо ознакомить строго ограниченный круг лиц, и документах, подлежащих направлению (передаче) лично адресатам, проставляется ограничительная пометка «Лично». При необходимости в документе указывается, кто из должностных лиц должен (может) быть ознакомлен с ним.

3.4. На обратной стороне последнего листа каждого экземпляра печатается разметка, в которой указывается: количество отпечатанных экземпляров, регистрационный номер, фамилия исполнителя и его телефон, дата и срок защиты (регистрационный номер проставляется на каждом листе документа).

3.5. Срок защиты конфиденциальной информации, содержащейся в документе на бумажном носителе, определяется в каждом конкретном случае исполнителем и утверждается руководством структурного подразделения в виде конкретной даты или в виде пометок: «до заключения контракта/договора», «бессрочно» и т. п. и личной подписи.

3.6. Основанием для снятия грифа «Конфиденциально» или «Коммерческая тайна» является решение руководства структурного подразделения, оформляемое актом, утвержденным руководителем Института. Один экземпляр акта вместе с делами передается в архив Института.

3.7. Гриф «Конфиденциально» или «Коммерческая тайна» после оформления его снятия (п. 2.4) погашается штампом или записью от руки с указанием даты и номера акта,

послужившего основанием для его снятия. Аналогичные отметки вносятся в описи дел (архивов).

4. Организация работы с документами на бумажном носителе, имеющих гриф «Конфиденциально» или «Коммерческая тайна»

4.1. Все входящие, исходящие и внутренние документы на бумажном носителе, имеющие гриф «Конфиденциально» или «Коммерческая тайна», подлежат обязательной регистрации у соответствующих секретарей в специальных регистрационных журналах и учитываются по количеству листов, а издания — поэкземплярно.

4.2. Права на информацию, порядок пользования ею, сроки ограничения на публикацию могут оговариваться дополнительно в тексте документа, его реквизитах или резолюциях.

4.3. Отсутствие грифа «Конфиденциально» или «Коммерческая тайна» и предупредительных оговорок в тексте и реквизитах означает свободную рассылку и предполагает, что автор информации и лицо, подписавшее или утвердившее документ, предусмотрели возможные последствия от свободной рассылки и несут за это ответственность.

4.4. Вся входящая корреспонденция, имеющая гриф «Конфиденциально» или «Коммерческая тайна» (или другие соответствующие этому понятию грифы, например «секрет предприятия», «тайна предприятия» и др.), вскрывается сотрудниками организации, имеющими соответствующий допуск и которым поручена работа с этими материалами. При этом проверяется количество листов и экземпляров, а также наличие указанных в сопроводительном письме приложений. Если обнаруживается отсутствие в конвертах (пакетах) указанных документов, составляется акт в двух экземплярах: один экземпляр акта направляется отправителю.

4.5. На рассмотрение руководства Института передаются все конфиденциальные документы на бумажном носителе, адресованные руководству Института, документы, по которым только руководство Института может назначить исполнителя, а также в случае, если документ адресован конкретному сотруднику, однако последний не имеет права доступа к данной категории документов.

4.6. Учет документов на бумажном носителе с грифом «Конфиденциально» или «Коммерческая тайна» ведется в регистрационных журналах отдельно от учета другой служебной документации, не имеющей ограничения по доступу. Листы регистрационных журналов нумеруются, прошиваются и опечатываются.

4.7. Проекты (черновики) конфиденциальных документов на бумажном носителе исполнителями составляются только в электронном виде с использованием электронных средств защиты или в специальных персональных тетрадях, указанных в пункте 4.15 данной Инструкции.

4.8. Конфиденциальные документы на бумажном носителе составляются в строго ограниченном количестве экземпляров. Исходящие документы на бумажном носителе составляются, как правило, в двух экземплярах, а внутреннего обращения — в одном.

4.9. Движение документов на бумажном носителе с грифом «Конфиденциально» или «Коммерческая тайна» осуществляется через соответствующих секретарей и только с помощью персонального реестра (с обязательной подписью исполнителя, получившего документ) и своевременно отражается в регистрационных журналах.

4.10. На зарегистрированном входящем документе на бумажном носителе с грифом, ограничивающим доступ к информации, должен быть проставлен штамп с указанием наименования организации, регистрационного номера документа и даты его поступления.

4.11. Отпечатанные и подписанные исходящие документы с грифом «Конфиденциально» или «Коммерческая тайна» передаются для регистрации секретарю руководителя организации (в случае, если исходящий документ подписан руководством Института) или секретарю руководителя структурного подразделения (в случае если исходящий документ подписан руководством структурного подразделения).

4.12. В случае, если исходящий конфиденциальный документ на бумажном носителе рассылается в несколько адресов, рассылка производится на основании подписанных руководством Института или руководством структурных подразделений разнарядок с указанием учетных номеров отправляемых экземпляров. Отправка по городу Новосибирску и в ближайшие регионы осуществляется только с помощью курьеров. В отдаленные регионы отправка данных документов осуществляется с помощью органов спецсвязи или фельдсвязи.

4.13. Размножение документов на бумажном носителе с грифом «Конфиденциально» или «Коммерческая тайна» на копировально-множительной технике производится только у соответствующих секретарей на основании вышеуказанных разнарядок или иных разрешений руководства Института или руководителей структурных подразделений.

Размноженные документы с грифом «Конфиденциально» или «Коммерческая тайна» (копии, тираж) должны быть полистно подобраны, пронумерованы поэкземплярно и, при необходимости, сброшюрованы (сшиты). Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенных экземпляров этого документа.

После размножения на последнем листе оригинала (подлинника) проставляется запись: «Регистрационный № _____. Дополнительно размножено _____ экз., на _____ листах текста. Должность, Ф. И. О. лица, разрешившего размножение. Дата. Подпись».

Одновременно делается отметка об этом в соответствующих регистрационных журналах.

4.14. Документы на бумажном носителе с грифом «Конфиденциально» или «Коммерческая тайна» после исполнения группируются в отдельные дела в хронологическом порядке.

4.15. Снятие рукописных, машинописных, микро- и фотокопий, электрографических и др. копий, а также производство выписок из документов с грифом «Конфиденциально» или «Коммерческая тайна» сотрудниками Института производится по разрешению руководства Института или руководства структурных подразделений. Данные выписки должны делаться в специальные персональные тетради, имеющие гриф «Конфиденциально» или «Коммерческая тайна», регистрационные номера, пронумерованные страницы, которые прошиты и скреплены печатью организации.

4.16. Печатание документов, содержащих конфиденциальную информацию, на бумажные носители разрешается у секретарей или непосредственно на рабочем месте исполнителя.

4.17. Уничтожение документов на бумажном носителе с грифом «Конфиденциально» или «Коммерческая тайна» производится комиссией в составе не менее трех человек с составлением соответствующего акта, при этом хотя бы один из них должен быть членом Постоянно действующей комиссии по защите конфиденциальной информации.

5. Порядок обеспечения сохранности документов и дел (архивов), содержащих конфиденциальную информацию

5.1. Все документы и дела (архивы) с документами, имеющими гриф «Конфиденциально» или «Коммерческая тайна», должны храниться в офисных помещениях в надежно запираемых и опечатываемых сейфах (металлических шкафах). Помещения должны отвечать требованиям

внутриобъектового режима, обеспечивающего физическую сохранность находящейся в них документации.

5.2. Дела (архивы) с документами, имеющими гриф «Конфиденциально» или «Коммерческая тайна», выдаются секретарями под роспись в регистрационном журнале и подлежат возврату сотрудниками в тот же день. При необходимости, с разрешения руководства структурного подразделения, они могут находиться у сотрудника в течение срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения надлежащих правил хранения.

5.3. С документами (электронными и бумажными) с грифом «Конфиденциально» или «Коммерческая тайна» разрешается работать только в офисных помещениях Института. Для работы вне офисных помещений необходимо разрешение руководства Института.

5.4. Во время перерывов в работе, связанных с выходом из своего офисного помещения, запрещается оставлять конфиденциальные документы на столах, в незапертых ящиках столов. В случае пребывания в офисном помещении посетителей или иных лиц, не имеющих допуск к данным конфиденциальным документам на бумажном носителе, все конфиденциальные документы должны быть убраны в сейфы (металлические шкафы).

5.5. Изъятия из дел (архивов) или перемещение документов на бумажном носителе с грифом «Конфиденциально» или «Коммерческая тайна» из одного дела (архива) в другое без санкции руководства Института или руководства структурных подразделений запрещается.

5.6. Смена секретарей, ответственных за учет и хранение документов, дел (архивов) с грифом «Конфиденциально» или «Коммерческая тайна», оформляется распоряжением руководства Института или руководства структурных подразделений. При этом составляется акт приема-передачи данных материалов, утверждаемый соответствующим руководством.

6. Порядок допуска к конфиденциальным сведениям

6.1. Допуск сотрудников к конфиденциальным сведениям осуществляется руководством Института и оформляется соответствующим решением в письменной форме.

6.2. Руководители структурных подразделений обязаны обеспечить систематический контроль за допуском к конфиденциальным сведениям только тех лиц, которым они необходимы для выполнения их функциональных обязанностей.

6.3. К конфиденциальным сведениям допускаются лица, личные и деловые качества которых обеспечивают их способность хранить конфиденциальную информацию, — и только после оформления письменного обязательства по сохранению конфиденциальной информации.

6.4. Допуск сотрудников к работе с делами (архивами), в которых хранятся конфиденциальные документы, осуществляется согласно оформленному на внутренней стороне обложки дела (архива) или на отдельном листе списку допущенных сотрудников за подписью руководства Института, а к документам — в соответствии с указаниями, содержащимися в резолюциях руководства Института или руководства структурных подразделений.

6.5. Представители сторонних организаций и частные лица могут быть допущены к ознакомлению и работе с документами и делами (архивами) с грифом «Конфиденциально» или «Коммерческая тайна» только с разрешения руководства Института.

6.6. Выписки из документов, содержащих сведения с грифом «Конфиденциально» или «Коммерческая тайна», производятся в специальных тетрадях, определенных в пункте 4.15 настоящей Инструкции. После окончания работы тетради высылаются в адрес той организации, которая будет указана уполномоченным лицом.

7. Контроль выполнения требований внутриобъектового режима при работе с конфиденциальными сведениями

7.1. Под внутриобъектовым режимом при работе с конфиденциальными документами подразумевается соблюдение условий работы, исключающих возможность утечки конфиденциальной информации.

7.2. Контроль соблюдения указанного режима осуществляется в целях изучения и оценки состояния сохранности конфиденциальной информации, выявления и установления причин недостатков, а также выработки предложений по их устранению.

7.3. Контроль обеспечения режима при работе с конфиденциальными сведениями осуществляют соответствующие сотрудники Научно-организационного отдела и руководители структурных подразделений путем текущих и внеплановых проверок.

7.4. При проведении проверок создается комиссия, которая комплектуется из сотрудников Научно-организационного отдела, экспертов Постоянно действующей комиссии по защите конфиденциальной информации и сотрудников организации, допущенных к работе с материалами, имеющими гриф «Конфиденциально» или «Коммерческая тайна», в общем составе не менее трех человек.

7.5. Участие в проверке не должно приводить к необоснованному увеличению осведомленности в защищаемых сведениях, а также затруднять работу сотрудников Института.

7.6. Плановые проверки проводятся не реже одного раза в 6 месяцев на основании распоряжения руководства Института.

7.7. Внеплановые проверки проводятся при наличии признаков утечки конфиденциальной информации или по иной необходимости на основании распоряжения руководителя Института по согласовании с Научно-организационным отделом.

7.8. Проверяющие имеют право знакомиться со всеми документами и иными материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы, консультироваться со специалистами и исполнителями, требовать представления письменных объяснений, справок и отчетов по всем вопросам, входящим в компетенцию комиссии.

7.9. При проверках может присутствовать руководство структурного подразделения.

7.10. По результатам проверок составляется акт или справка с отражением в нем наличия документов, состояния работы с материалами, имеющими гриф «Конфиденциально» или «Коммерческая тайна», выявленных недостатков и предложений по их устранению. Акт подписывается начальником Научно-организационного отдела и утверждается руководством Института.

7.11. При выявлении случаев утраты документов или разглашения конфиденциальных сведений ставятся в известность руководитель Института и начальник Научно-организационного отдела. Для расследования указанных случаев распоряжением руководителя Института Постоянно действующая комиссия по защите конфиденциальной информации определяет соответствие содержания утраченного документа проставленному грифу «Конфиденциально» или «Коммерческая тайна» и выявляет обстоятельства утраты (разглашения), а также формирует предложения по минимизации убытков, связанных с утратой документа или разглашением конфиденциальной информации. По результатам работы комиссии составляется акт.

8. Обязанности сотрудников Института, работающих с конфиденциальными сведениями, и их ответственность за разглашение таких сведений

8.1. Сотрудники организации, допущенные к конфиденциальными сведениям, несут ответственность за неточное выполнение требований, предъявляемых к ним (сведениям) в целях обеспечения сохранности указанных сведений.

8.2. До получения доступа к работе, связанной с конфиденциальной информацией, сотрудникам необходимо изучить настоящую Инструкцию под роспись и заключить письменное обязательство о сохранении конфиденциальной информации в установленном порядке.

8.3. Сотрудники Института, допущенные к конфиденциальной информации, должны:

- знать и соблюдать требования настоящей Инструкции;
- хранить конфиденциальную информацию, в т. ч. не сообщать конфиденциальные сведения друзьям и членам семьи. О ставших им известной утечке сведений, составляющих конфиденциальную информацию, а также об утрате документов с грифом «Конфиденциально» или «Коммерческая тайна», немедленно сообщать руководителю своего структурного подразделения и в Научно-организационный отдел;
- предъявлять для проверки по требованию комиссии по проверке конфиденциального делопроизводства и представителей Научно-организационного отдела все числящиеся за ним материалы, содержащие конфиденциальную информацию, а в случае нарушения установленных правил работы с ними представлять соответствующие объяснения в устном и письменном виде;
- знакомиться только с теми документами и выполнять только те работы, к которым они допущены в соответствии с функциональными обязанностями и в соответствии с дополнительными задачами, возложенными на них руководством;
- строго соблюдать правила пользования и сохранности документов, имеющих гриф «Конфиденциально» или «Коммерческая тайна». Не допускать их необоснованной рассылки;
- выполнять требования внутриобъектового режима, определяемые Научно-организационным отделом, исключающие возможность ознакомления с материалами, содержащими конфиденциальную информацию, посторонних лиц, включая сотрудников организации, не имеющих к указанным материалам прямого отношения.
- при ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения;
- при временном убытии (в отпуск, командировку, на учебу, лечение и т. д.) проверять наличие числящихся за ним конфиденциальных документов. Документы, которые подлежат исполнению или могут потребоваться в работе, передавать другому сотруднику по указанию руководства Института или руководства структурного подразделения. При прекращении трудовых или иных договорных отношений с Институтом сотрудник обязан сдать все числящиеся за ним конфиденциальные документы;
- исключить использование конфиденциальных сведений в свою личную пользу, а также исключить участие в деятельности, которая может быть использована конкурентами в ущерб Институту.

8.4. Ответственность за разглашение конфиденциальных сведений и утрату документов, содержащих такие сведения, устанавливается в соответствии с Уголовным кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Трудовым кодексом Российской Федерации и иными нормативными актами.

Заместитель директора
по научной работе, к.х.н. В.В. Коваль
09.01.2019 г.
Согласовано:
Юрисконсульт А.А. Конопацкий
Ученый секретарь, к.х.н. П.Е. Пестряков

Заведующий ОИТНО А.П. Зенков

Ведущий инженер НОО
(секретарь директора) М.С. Кшнякина