

САНКТ-ПЕТЕРБУРГСКОЕ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ

«МЕДИЦИНСКИЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР»

**П Р И К А З**

от « » \_\_\_\_\_\_\_\_\_\_\_\_\_\_2018 г. №\_\_\_\_\_\_\_\_\_

**Об утверждении инструкций**

**по защите персональных данных**

Во исполнение Федерального закона Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и прочих нормативных документов по защите информации, а также с целью обеспечения безопасности персональных данных в СПб ГБУЗ МИАЦ,

**ПРИКАЗЫВАЮ:**

1. Утвердить и ввести в действие Инструкцию по парольной защите информации в СПб ГБУЗ МИАЦ (Приложение 1 к настоящему приказу).
2. Утвердить и ввести в действие Инструкцию по организации антивирусной защиты информации в СПб ГБУЗ МИАЦ (Приложение 2 к настоящему приказу).
3. Утвердить и ввести в действие Инструкцию о порядке использования информационно-телекоммуникационных сетей международного информационного обмена и электронной почты (Приложение 3 к настоящему приказу).
4. Утвердить и ввести в действие Инструкцию о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных СПб ГБУЗ МИАЦ (Приложение 4 к настоящему приказу).
5. Требования настоящего приказа довести до работников, осуществляющих обработку персональных данных в информационных системах персональных данных в СПб ГБУЗ МИАЦ.
6. Контроль над исполнением настоящего приказа возложить на заместителя директора по информационным технологиям А.А. Гребенщикова.

**Директор \_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Д. А. Яценко**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Приложение 1  к приказу СПб ГБУЗ МИАЦ  от «\_\_\_» \_\_\_\_\_\_ 2018 г. № \_\_\_  **ИНСТРУКЦИЯ**  **по парольной защите информации в СПб ГБУЗ МИАЦ**   1. **Термины и определения**   Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;  Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;  Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;  Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;  Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);  Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных;  Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.   1. **Общие положения** 2. Настоящая Инструкция по парольной защите информации в СПб ГБУЗ МИАЦ (далее – Инструкция) устанавливает требования и ответственность при организации парольной защиты информации, а также определяет порядок контроля за действиями пользователей и обслуживающего персонала информационных систем персональных данных (далее – ИСПДн) при работе с паролями. 3. Требования настоящей Инструкции являются обязательными для исполнения всеми пользователями и администраторами СПб ГБУЗ МИАЦ (далее – Учреждение), использующими в своей работе средства вычислительной техники. 4. Все пользователи и администраторы Учреждения, использующие в своей работе средства вычислительной техники, должны быть ознакомлены с требования настоящей Инструкции под подпись. 5. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований. 6. **Требования, предъявляемые к идентификаторам (кодам) и паролям (порядок формирования и обращения с ними)** 7. Авторизация пользователей на средствах вычислительной техники в сети Учреждения осуществляется путем ввода идентификатора и/или пароля. 8. Требования к формированию паролей и обращению с ними: 9. Пароль формируется при создании учетной записи администратором безопасности. 10. Владельцы личных паролей обязаны обеспечить их тайну. 11. Пароли генерируются с учетом следующих требований:  * пароль должен знать только его владелец; * длина пароля должна быть не менее 10 символов и генерироваться автоматически с использованием специальных генераторов паролей; * пароль не может содержать имя учетной записи пользователя или какую-либо его часть; * в пароле должны присутствовать символы следующих категорий: * прописные буквы английского алфавита от A до Z; * строчные буквы английского алфавита от a до z; * десятичные цифры (от 0 до 9); * символы, не принадлежащие алфавитно-цифровому набору (знаки препинания, скобки, символы $%^&\*@%-+= и другие). * в составе символов пароля обязательно должны присутствовать как цифры, буквы на верхнем и нижнем регистрах так и символ; * пароль не должен включать смысловую нагрузку (имена, фамилии, наименования организаций, улиц, городов и т.д.), общепринятые сокращения (userOl, password02 и т.п.) и последовательные сочетания клавиш клавиатуры (qwertyOl, Ицукен12); * количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя должно быть не более 5.  1. Требования к формированию паролей обеспечиваются техническими возможностями используемых операционных систем, средств защиты информации и информационных ресурсов. 2. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода. Внеплановая смена пароля производится в случае его компрометации, а также по просьбе пользователя ИСПДн. 3. Хранение пользователями ИСПДн значений своих паролей на бумажном носителе ЗАПРЕЩЕНО. 4. Порядок смены паролей и идентификаторов при изменениях в организационно-штатной структуре (кадровые перестановки, увольнение работников): 5. При прекращении действия трудового договора с работником все созданные для этого работника учетные записи (пользовательское имя) подлежат блокированию не позднее, чем в день увольнения работника. Полное удаление учетных записей производится в течение 5 рабочих дней со дня увольнения работника. Основанием для блокирования и последующего удаления учетных записей работника является заявка, представленная непосредственным руководителем увольняемого не позднее, чем за 3 рабочих дня до дня его увольнения. 6. При проведении организационно-штатных мероприятий (кадровые перестановки) непосредственный руководитель структурного подразделения обязан представить администратору безопасности заявку на изменение в правах доступа. 7. Порядок действий при компрометации идентификаторов и паролей. 8. Под компрометацией понимается: утрата пароля учетной записи и (или) пароля идентификатора, разглашение учетной записи пароля или пароля идентификатора (явная компрометация), или иная ситуация, которая дает основание для предположения о нарушении конфиденциальности паролей и идентификаторов (неявная компрометация). 9. При выявлении факта утраты пароля, разглашения пароля, пароля идентификатора, самого идентификатора пользователь обязан незамедлительно сообщить о данных фактах своему непосредственному руководителю и администратору безопасности. 10. В случае выявления факта компрометации идентификаторов и паролей пользователя администратор безопасности обязан немедленно заблокировать учетную запись данного пользователя и незамедлительно произвести внеплановую смену пароля для этого пользователя. 11. Для администратора безопасности обязательно выполнение п. 4.7 «Реализация парольной защиты» документа «Руководство администратор безопасности». 12. **Права и обязанности** 13. Основные задачи администратора безопасности:  * организация установки средств идентификации и аутентификации; * организация парольной защиты в Учреждении; * выдача первичных паролей, и электронных персональных идентификаторов и паролей к ним; * осуществление контроля за состоянием системы парольной защиты информации в ИСПДн Учреждения.  1. Администратор безопасности имеет право:  * вносить предложения по совершенствованию системы парольной защиты информации в Учреждении; * принимать участие в планировании мероприятий по парольной защите информации в Учреждении и планировании оснащения средствами идентификации и аутентификации; * осуществлять контроль состояния средств идентификации и аутентификации в Учреждении; * инициировать служебные проверки и участвовать в проведении расследований по фактам компрометации; * оказывать помощь в решении проблем, возникающих при эксплуатации средств идентификации и аутентификации.  1. Обязанности в части парольной защиты информации отражены в инструкции администратора безопасности. 2. Пользователям ИСПДн в своей работе запрещается:  * сообщать кому-либо свой личный пароль и/или пароль к электронному персональному идентификатору; * передавать кому-либо выданный электронный персональный идентификатор; * осуществлять вход в операционные системы ИСПДн и в информационные ресурсы под чужими идентификаторами и паролями; * отключать средства идентификации и аутентификации.  1. В случае появления подозрений на факт компрометации пароля, а также в случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств идентификации и аутентификации, пользователи обязаны немедленно проинформировать об этом ответственного за обеспечение безопасности ПДн в ИСПДн или администратора безопасности. 2. **Ответственность должностных лиц в рамках системы парольной защиты информации** 3. Пользователи, ответственные за обеспечение безопасности ПДн в ИСПДн и администратор безопасности несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность. 4. Пользователи, ответственные за обеспечение безопасности ПДн в ИСПДн и администратор безопасности несут ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией. 5. **Срок действия и порядок внесения изменений**    1. Инструкция вступает в силу с момента его утверждения и действует бессрочно.    2. Инструкция подлежит пересмотру не реже одного раза в три года.    3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.   Приложение 2  к приказу СПб ГБУЗ МИАЦ  от «\_\_\_» \_\_\_\_\_\_\_ 2018 г. № \_\_\_  **ИНСТРУКЦИЯ**  **по антивирусной защите СПб ГБУЗ МИАЦ**   1. **Термины и определения**   Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;  Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование "зараженных" объектов, удаление вредоносных компьютерных программ (вирусов) из "зараженных" объектов);  Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;  Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;  Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;  Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);  Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных;  Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации;  Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.   1. **Общие положения** 2. Инструкция по антивирусной защите СПб ГБУЗ МИАЦ (далее – Инструкция) регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля. 3. Инструкция устанавливает требования и ответственность при организации защиты информации от разрушающего воздействия вредоносных программ – компьютерных вирусов. 4. Требования настоящей Инструкции являются обязательными для исполнения всеми работниками СПб ГБУЗ МИАЦ (далее – Учреждения), использующими в своей работе средства вычислительной техники. 5. Все работники Учреждения, использующие антивирусные средства, должны быть ознакомлены с требованиями настоящей Инструкцией под подпись. 6. Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований. 7. **Требования к антивирусным средствам** 8. В Учреждении к применению допускаются только лицензионные антивирусные программные и (или) программно-аппаратные средства (антивирусные средства), закупленные у разработчика указанных средств или его официальных дилеров. 9. Антивирусные средства должны функционировать в течение всего времени работы средств вычислительной техники (от момента загрузки операционной системы до момента ее выгрузки). 10. Антивирусное средство не должно существенно затруднять работоспособность средств вычислительной техники информационных систем персональных данных (далее – ИСПДн). 11. **Права и обязанности** 12. Антивирусной защите подлежит вся, обрабатываемая в Учреждении при помощи средств вычислительной техники, информация (сервера, автоматизированные рабочие места (АРМ) пользователей), независимо от ограничений доступа к ней. 13. Сопровождение (регулярное обновление, антивирусный контроль, выявление фактов заражения и проведение служебных расследований) правил антивирусной защиты возлагаются на администратора безопасности. 14. Основные задачи администратора безопасности:  * организация процесса установки антивирусных средств в ИСПДн; * сопровождение антивирусных средств (обновление, антивирусный контроль, сопровождение действий пользователей в случаях обнаружения вирусов, обеспечение работоспособности антивирусных средств); * контроль состояния системы антивирусной защиты информации в Учреждении; * обязательное выполнение п. 4.9. «Проведение антивирусного контроля» документа «Руководство администратора безопасности».  1. Администратор безопасности несет ответственность за:  * за своевременную установку антивирусных средств; * за эксплуатацию (антивирусный контроль, работоспособность антивирусных средств, сопровождение действий пользователей в случаях обнаружения вирусов) системы антивирусной защиты информации; * за своевременное обновление лицензий на антивирусные средства; * за своевременное обновление антивирусных баз.  1. Администратор безопасности имеет право:  * вносить предложения по совершенствованию системы антивирусной защиты информации; * принимать участие в планировании мероприятий по антивирусной защите информации и планировании оснащения антивирусными средствами; * осуществлять контроль состояния средств антивирусной защиты информации в Учреждении; * инициировать служебные проверки и участвовать в проведении расследований по фактам заражения вирусами ИСПДн и средств вычислительной техники; * оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты.  1. Пользователь антивирусного средства – лицо, на рабочем месте которого применяется антивирусное средство. 2. Пользователям антивирусных средств запрещается:  * менять настройки или отключать средства антивирусной защиты во время работы; * использовать средства антивирусной защиты, отличные от установленных средств; * без разрешения ответственного за обеспечение безопасности ПДн в ИСПДн и администратора безопасности копировать любые файлы на съемные носители информации, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.  1. **Порядок и периодичность обновления антивирусных баз** 2. Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации. 3. Установке обновлений должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий от вновь устанавливаемых обновлений. 4. Установке новых версий программного обеспечения или внесению изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование ИСПДн на отсутствие негативных воздействий указанного программного обеспечения. 5. Периодичность обновления антивирусных баз:  * обновление антивирусных баз для всех АРМ пользователей, имеющих подключение к сетям общего пользования и сетям международного информационного обмена, должно быть ежедневным. Источник обновления – сервер разработчика антивирусного средства, либо собственный централизованный сетевой источник обновлений, получающий обновления с сервера разработчика антивирусного средства. * обновление антивирусных баз для АРМ пользователей, не имеющих подключение к сетям общего пользования и сетям международного информационного обмена, обновление должно быть не менее 1 раза в неделю. Источником обновления в данном случае являются антивирусные базы, записанные на предварительно учтенный в установленном порядке съемный машинный носитель информации.  1. **Порядок и периодичность проведения антивирусного контроля** 2. Объектами антивирусного контроля являются:  * жесткие магнитные диски рабочих станций и серверов ИСПДн; * сетевые хранилища (системы хранения данных); * оперативная и системная память средств вычислительной техники; * съемные машинные носители информации; * входящий и исходящий контент (веб-трафик); * файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена; * почтовые сообщения электронной почты.  1. Антивирусный контроль входящей информации со съемных машинных носителей информации необходимо проводить до переноса информации на жёсткий магнитный диск рабочей станции или сетевой диск. Информация, получаемая по телекоммуникационным каналам, должна проверятся во время, или сразу после получения. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель). 2. Виды и периодичность антивирусных проверок представлены в таблице 1.   Таблица 1   | № п/п | Объект контроля | Вид проверки | Периодичность проверки | | --- | --- | --- | --- | | 1 | Жесткие магнитные диски рабочих станций и серверов ИСПДн | Полная проверка | 1 раз в месяц | | Быстрое сканирование | 1 раз в неделю | | 2 | Сетевые хранилища (системы хранения данных) | Полная проверка | 1 раз в месяц | | 3 | Оперативная и системная память средств вычислительной техники | Полная проверка | 1 раз в месяц | | Быстрое сканирование | 1 раз в неделю | | 4 | Съемные машинные носители информации | Полная проверка | При каждом подключении | | 5 | Веб-трафик | Минимально необходимое требование -  настройка антивирусного средства по умолчанию | Постоянно | | 6 | Файлы, получаемые и передаваемые через сети общего пользования и международного информационного обмена | Полная проверка | При каждом получении и отправке | | 7 | Почтовые сообщения электронной почты | Минимально необходимое требование -  настройка антивирусного средства по умолчанию | При каждом получении и отправке |  1. **Порядок действий при обнаружении вирусов** 2. Основными путями проникновения вирусов на АРМ пользователей являются: любые съемные машинные носители информации, электронные почтовые сообщения, трафик, получаемый из сетей общего пользования и сетей международного информационного обмена, ранее зараженные рабочие станции и сервера. 3. В случае обнаружения вирусов при входном контроле съемных машинных носителей информации, файлов или электронных почтовых сообщений, пользователь должен:  * немедленно приостановить все работы на своей рабочей станции; * сообщить администратору безопасности о факте обнаружения вируса; * принять согласованные с ответственным за обеспечение безопасности ПДн в ИСПДн или с администратором безопасности меры по локализации и удалению вируса с использованием антивирусных средств.  1. При невозможности ликвидации последствий вирусного заражения администратору безопасности необходимо:  * сообщить о факте обнаружения программных вирусов в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации; * заархивировать зараженные файлы и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации.  1. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению администратора по безопасности или ответственного за обеспечение безопасности ПДн в ИСПДн. 2. Факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ – все это относится к значимым нарушениям безопасности информации и должны быть проанализированы посредством проведения служебного расследования. 3. Служебное расследование проводится комиссией, назначаемой приказом директора Учреждения. В состав комиссии в обязательном порядке включается администратор безопасности ИСПДн, ответственный за обеспечение безопасности ПДн в ИСПДн, непосредственный руководитель работника, допустившего факт компрометации. При необходимости в состав комиссии могут включаться другие сотрудники. 4. Результаты работы комиссии оформляются актом. Акт подлежит утверждению директора Учреждения. 5. В процессе работы комиссии обязательными для установления являются:  * дата и время заражения (обнаружения заражения); * ФИО, должность и подразделение сотрудника, техническое средство которого заражено вирусной программой; * уровень критичности заражения; * обстоятельства, способствовавшие заражению; * информационные ресурсы, затронутые заражением; * характер и размер реального и потенциального ущерба.  1. В ходе своей работы комиссия может запрашивать объяснительные записки от работников, подозреваемых в виновности заражения (путем письменного запроса их непосредственным руководителям). Объяснительная записка должна быть представлена комиссии в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа предоставить объяснительную записку, данный факт отражается в акте. 2. Уничтожение материалов расследования фактов заражения осуществляется в соответствии с установленными требованиями по делопроизводству и номенклатурой дел. 3. **Ответственность** 4. Пользователи и ответственный за обеспечение безопасности ПДн в ИСПДн (в том числе администратор безопасности) несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность. 5. **Срок действия и порядок внесения изменений** 6. Инструкция вступает в силу с момента его утверждения и действует бессрочно. 7. Инструкция подлежит пересмотру не реже одного раза в три года. 8. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.   Приложение 3  к приказу СПб ГБУЗ МИАЦ  от «\_\_\_» \_\_\_\_\_\_\_ 2018 г. № \_\_\_  **ИНСТРУКЦИЯ**  **о порядке использования информационно-телекоммуникационных сетей международного информационного обмена и электронной почты**   1. Общие положения   Инструкция разработана на основании Федерального закона "Об информации, информационных технологиях и о защите информации" от 27.07.2006 №149-ФЗ, «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 09.09.2000 № Пр-1895, «Специальных требований и рекомендаций по защите конфиденциальной информации» (СТР-К) утвержденных приказом Гостехкомиссии России 30.08.2002 № 282, Указа Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 № 351 и других нормативных правовых документов в области защиты информации.  Настоящая инструкция определяет основные требования по организации работы в области защиты информации, общий порядок обращения с документами и другими материальными носителями информации при подключении и использовании информационно-телекоммуникационных сетей международного информационного обмена и электронной почты, в Санкт-Петербургском государственном бюджетном учреждении здравоохранения «Медицинский информационно-аналитический центр» (далее – СПб ГБУЗ МИАЦ).   1. Источники угроз информационной безопасности   Подключение средств вычислительной техники к информационно-телекоммуникационным сетям международного информационного обмена представляет реальную угрозу создания разветвленных систем регулярного несанкционированного контроля информационных процессов и ресурсов, несанкционированного доступа (НСД) в автоматизированные системы (АС).  Информационные вычислительные сети общего пользования являются открытыми системами передачи информации, при работе в которых могут возникнуть следующие основные угрозы безопасности информации:   * проникновение в систему незаконных пользователей, которое происходит вследствие ошибок в конфигурации программных средств (ошибок администрирования), дефектов в средствах обеспечения защиты информации от НСД операционных систем; * перенос в АС разрушающего программного обеспечения (внедрение программных закладок, вирусов); * выбор и использование законным пользователем системы неудачных паролей; * несанкционированная передача служебной информации ограниченного распространения пользователями в МИС общего пользования и т.д.  1. Работа в сети Интернет   Доступ пользователей к сети Интернет ограничен и лимитирован. Работа в сетях общего доступа и (или) международного обмена (далее - сеть Интернет, Сеть) должна проводиться при служебной необходимости по служебной записке руководителя соответствующего структурного подразделения.   * 1. Пользователи используют поиск информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей.   2. По использованию пользователями ресурсов сети Интернет ведется статистика, которая хранится на сервере.   3. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему санкций.   4. Работникам, пользующимся Интернетом, запрещено: * посещать сайты сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие); * передавать или загружать на компьютер материалы, которые являются непристойными, порнографическими или нарушают действующее законодательство Российской Федерации; * осуществлять работу при отключенных средствах защиты (антивирус и др.); * передавать по Сети информацию конфиденциального характера без использования средств защиты каналов связи; * скачивать из Сети программное обеспечение и другие развлекательные файлы; * использовать подключение к Сети по нецелевому назначению (online-игры, фильмы, интернет-магазины и т.д.); * распространять противозаконные материалы.   1. При необходимости загрузки рабочих материалов, полученных из сети Интернет, на рабочий компьютер пользователя, требуется их проверка при помощи антивирусных программ, согласно Инструкции по организации антивирусной защиты в Учреждении.   2. Работники, обязаны: * строго соблюдать все правила данной политики после предоставления им доступа к сети Интернет; * хранить в тайне свой аутентификатор (пароль доступа), а так же информацию о системе защиты установленной в автоматизированной системе. * немедленно ставить в известность администратора безопасности и прекратить какие-либо действия на АРМ в случае обнаружения на АРМ сообщения об угрозе заражения вредоносным программным обеспечением; * строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС.  1. Порядок осуществления доступа и обмена данными с внешними информационными ресурсами и по электронной почте    1. Установка и настройка программного обеспечения для работы с электронной почтой или ресурсами сети Интернет осуществляется системным администратором отдела информационных технологий. Пользователям запрещается изменение любых параметров, касающихся способов подключения и используемых протоколов.    2. При работе с электронной почтой или ресурсами сети Интернет пользователям запрещается:  * обмен информацией для служебного пользования, а также информацией ограниченного доступа (в том числе персональными данными), по электронной почте или с использованием ресурсов сети Интернет; * предоставлять доступа к электронной почте или к ресурсам сети Интернет с использованием данных своей учетной записи другим лицам; * публиковать свой служебный адрес электронной почты в электронных каталогах, на поисковых машинах и других ресурсах сети Интернет в целях, не связанных с исполнением своих должностных обязанностей; * подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т.д., не связанные с выполнением пользователем должностных обязанностей, с целью предотвращения заполнения почты ненужной почтовой (рекламной и др.) информацией – спамом; * передавать сведения при пользовании электронной почтой, содержащие конфиденциальную информацию без применения специальных мер защиты (сертифицированных средств криптографической защиты информации); * копировать или распространять информацию с нарушением авторских прав или условий программных лицензий; * открытие (запуск на выполнение) файлов, полученных по электронной почте или из ресурсов сети Интернет, без предварительной проверки их антивирусным программным обеспечением.   1. Электронная почта предоставляется работникам только для выполнения своих прямых служебных обязанностей по служебной записке руководителя соответствующего структурного подразделения. Использование ее в личных целях запрещено. Создание почтового ящика проводится отделом по информационным технологиям по заявке, согласованной с руководителя соответствующего структурного подразделения.   2. Ответственный за информационную безопасность в ИСПДн совместно с администратором по безопасности оставляют за собой право получить доступ к электронной почте работников, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.   3. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности.   4. Пользователи не должны позволять кому-либо посылать письма от чужого имени.   5. В качестве клиентов электронной почты могут использоваться только согласованные c отделом информационных технологий почтовые программы.  1. Ответственность    1. Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере.    2. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в сети и за ее пределами.    3. За бесперебойное функционирование сети Интернет отвечает отдел информационных технологий, за качество предоставляемых пользователям сервисов отвечает провайдер, с которым у учреждения заключен договор на оказание услуг связи сети Интернет.    4. За нарушение настоящей инструкции пользователь может быть отстранен от работы в сети. 2. Срок действия и порядок внесения изменений 3. Инструкция вступает в силу с момента его утверждения и действует бессрочно. 4. Инструкция подлежит пересмотру не реже одного раза в три года. 5. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.   Приложение 4  к приказу СПб ГБУЗ МИАЦ  от «\_\_\_» \_\_\_\_\_\_\_ 2018 г. № \_\_\_  **ИНСТРУКЦИЯ**  **о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных**   1. **Термины и определения**   Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;  Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;  Инцидент – некоторое происшествие, связанное со сбоем в функционировании элементов информационной системы персональных данных (далее – ИСПДн), предоставляемых пользователям ИСПДн, а также потеря защищаемой информации;  Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;  Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;  Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);  Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных;  Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации;  Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.   1. **Общие положения** 2. Инструкция по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных СПб ГБУЗ МИАЦ (далее – Инструкция) устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных информационных систем персональных данных (далее – ИСПДн) СПб ГБУЗ МИАЦ (далее – Учреждение), а также к резервированию аппаратных средств. 3. Инструкция разработана с целью:  * определения категории информации, подлежащей обязательному резервному копированию; * определения процедуры резервирования данных для последующего восстановления работоспособности ИСПДн при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.); * определения порядка восстановления информации в случае возникновения такой необходимости; * упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.  1. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн Учреждения, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:  * системы жизнеобеспечения технических средств; * системы обеспечения отказоустойчивости; * системы резервного копирования и хранения данных;  1. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИСПДн в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных. 2. Резервному копированию подлежит информация следующих основных категорий:  * информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления базами данных (далее – СУБД) общего пользования и справочно-информационных систем общего использования; * рабочие копии установочных компонентов программного обеспечения общего назначения и специализированного программного обеспечения серверов и рабочих станций; * информация, необходимая для восстановления серверов и систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота; * регистрационная информация систем защиты информации; * другая информация ИСПДн, по мнению пользователей, администраторов ИСПДн и ответственного за обеспечение безопасности персональных данных (далее – ПДн) в ИСПДн, являющаяся критичной для работоспособности ИСПДн.  1. Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований. 2. **Общие требования к резервному копированию** 3. В Инструкции резервного копирования описываются действия при выполнении следующих мероприятий:  * резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости); * контроль резервного копирования; * хранение резервных копий; * полное или частичное восстановление данных.  1. Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования. Система резервного копирования должна обеспечить производительность, достаточную для сохранения информации, указанной в п. 2.5, в установленные сроки и с заданной периодичностью. 2. Для администратора безопасности обязательно к выполнению п. 4.5 «Порядок проведения процедуры резервного копирования, хранения и восстановления информации из резервных копий» документа «Руководство администратора безопасности». 3. При необходимости восстановления информации из архивной копии пользователь обращается к Администратору безопасности. После ознакомления с запросом Администратор безопасности принимает решение о возможности восстановления резервной копии. 4. Хранение отдельных магнитных носителей архивных копий организуется в отдельном хранилище. Физический доступ к архивным копиям строго ограничен. 5. Доступ к носителям архивных копий имеют только уполномоченные сотрудники, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то полномочий. 6. Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательным составлением акта об уничтожении. 7. **Ответственность за состояние резервного копирования** 8. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующей Инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности. 9. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается администратору безопасности информации в течение рабочего дня после обнаружения указанного события. 10. **Периодичность резервного копирования** 11. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий. 12. Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц. 13. Информация, содержащаяся в постоянно изменяемых базах данных, сохраняется в соответствии со следующим графиком:  * ежедневно проводится копирование измененной и дополненной информации (носители с ежедневной информацией должны храниться в течение недели); * еженедельно проводится резервное копирование всей базы данных (носители с еженедельными копиями хранятся в течение месяца); * ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.  1. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.). 2. **Восстановление информации из резервных копий** 3. В случае необходимости, восстановление данных из резервных копий производится ответственными сотрудниками. 4. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев. 5. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя. 6. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения. 7. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации. 8. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями. 9. **Срок действия и порядок внесения изменений** 10. Инструкция вступает в силу с момента его утверждения и действует бессрочно. 11. Инструкция подлежит пересмотру не реже одного раза в три года. 12. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.   ЛИСТ СОГЛАСОВАНИЯ  с приказом СПб ГБУЗ МИАЦ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2018 г. № \_\_\_\_\_\_  «Об утверждении инструкций по защите персональных данных»   |  |  |  |  |  | | --- | --- | --- | --- | --- | | № п/п | Фамилия имя отчество | Должность | Дата согласования | Подпись | | 1 | Гребенщиков А.А. | Зам. директора по инф.технологиям | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 2 | Целовальников Д.В. | Начальник ОИТ (ответственный за организацию обработки ПДн, администратор безопасности) | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 3 | Мартюшева Ю.Б. | Инженер по ЗИ (ответственный за обеспечение безопасности ПДн в ИСПДн) | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 4 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 5 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |   ЛИСТ ОЗНАКОМЛЕНИЯ  с приказом СПб ГБУЗ МИАЦ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2018 г. № \_\_\_\_\_\_  «Об утверждении инструкций по защите персональных данных»   |  |  |  |  |  | | --- | --- | --- | --- | --- | | № п/п | Фамилия имя отчество | Должность | Дата ознакомления | Подпись | | 1 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 2 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 3 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 4 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 5 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 6 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 7 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 8 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 9 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 10 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 11 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 12 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 13 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 14 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 15 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 16 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 17 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 18 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 19 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 20 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 21 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | | 22 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  | |