Одобрено на заседании

Совета по вопросам технической защиты информации

в Ханты-Мансийском автономном округе – Югре

Протокол от 29.05.2017 № 3/17

Типовые функции и задачи работников, эксплуатирующих информационную систему обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные в исполнительном органе государственной власти (органе местного самоуправления)

Ханты-Мансийского автономного округа – Югры

**1.Общие положения**

1. Настоящий документ определяет основные обязанности, права и ответственность работников, эксплуатирующих информационную систему исполнительного органа государственной власти Ханты-Мансийского автономного округа – Югры (далее – Пользователь) информационных систем обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные (далее – ИС) исполнительного органа государственной власти Ханты-Мансийского автономного округа – Югры (далее – орган власти).

2. Пользователем ИС является работник органа власти, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС, в соответствии со Списком лиц, допущенных к самостоятельной работе в ИС.

3. Пользователь должен принимать все необходимые меры по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных (далее – конфиденциальная информация (КИ)) и контролю за соблюдением прав доступа к ней.

4. Положения настоящего документа обязательны для исполнения всеми пользователями.

Все пользователи должны быть ознакомлены под роспись с настоящим документом и предупреждены об индивидуальной ответственности за его нарушения.

5. Основными задачами при обработке информации в ИС являются:

обеспечение исполнения требований нормативных правовых актов, руководящих документов, регламентирующих защиту информации в Российской Федерации в процессе создания, хранения и передачи документов, содержащих конфиденциальную информацию в ИС органа власти;

обеспечение в ИС необходимого уровня безопасности обработки, хранения и передачи КИ;

обеспечение необходимого уровня безопасности носителей КИ;

обеспечение безопасности конфиденциальной информации при ее копировании, размножении;

резервное копирование, восстановление информации.

**2. Основные положения**

6. При первичном допуске к работе в ИС пользователь изучает требования настоящего документа, разрешительную систему доступа к ИС, технологический процесс обработки информации в ИС, руководящие, нормативно-методические и организационно-распорядительные документы по вопросам обеспечения безопасности обрабатываемой информации.

7. Каждый пользователь ИС, имеющий в рамках своих обязанностей доступ к аппаратным средствам, программному обеспечению и данным ИС, несет персональную ответственность за свои действия и **обязан**:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС, в том числе положения настоящего документа;

знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;

располагать основные технические средства и системы (далее – ОТСС) в соответствии с техническим паспортом;

хранить в тайне свой пароль (пароли), парольную защиту организовывать в соответствии с инструкцией по организации парольной защиты;

выполнять требования «Инструкции по организации антивирусной защиты»;

немедленно вызывать администратора безопасности и ставить в известность руководителя подразделения при подозрении компрометации личных ключей и паролей или при обнаружении фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к основным техническим средствам и системам (далее – ОТСС) ИС;

в случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах или попытках НСД к информации, обрабатываемой в ИС, пользователь должен немедленно сообщить об этом администратору безопасности;

немедленно сообщать администратору информационной безопасности об обнаруженных фактах нарушения информационной безопасности кем-либо;

сообщать администратору информационной безопасности об отклонениях в нормальной работе установленных на рабочей станции средств защиты информации;

при работе в ИС выполнять только служебные задания;

при отсутствии необходимости работы выключить (блокировать) компьютер;

при работе в ИС использовать только учтенные съемные носители, при обоснованной необходимости использования неучтённых носителей согласовывать использование с администратором информационной безопасности. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;

осуществлять установленным порядком уничтожение информации (сочетанием клавиш Shift+Del), содержащей сведения конфиденциального характера, с машинных (съемных) носителей информации;

немедленно выполнять предписания администратора безопасности в части обеспечения безопасности информации;

экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;

соблюдать установленный режим разграничения доступа к информационным ресурсам;

не разглашать известную им информацию, составляющую конфиденциальную информацию лицам, не имеющим допуска к этой информации;

все изменения конфигурации технических и программных средств ИС, ремонт, модификация и техническое обслуживание технических средств и систем, входящих в состав ИС производить только на основании «Инструкции пользователю по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств».

8. Пользователю запрещается:

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств, устанавливать или удалять установленные техническим специалистом (администратором информационной безопасности) сетевые программы на компьютерах, вскрывать компьютеры, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование, вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства без согласования с администратором безопасности;

привлекать посторонних лиц для производства ремонта ОТСС без письменной заявки и согласования с администратором информационной безопасности;

запускать любые системные или прикладные программы, не входящие в состав программного обеспечения;

работать с неучтенными машинными (съемными) носителями информации;

отключать (блокировать) средства защиты информации;

производить какие-либо изменения в размещении технических средств;

обрабатывать на средствах вычислительной техники (далее – СВТ) входящих в состав ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам;

сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ИС;

хранить на учтенных носителях программы и данные, не относящиеся к рабочей информации;

выполнять работы с документами ограниченного распространения на дому, выносить их за пределы контролируемой зоны;

передавать свои учтённые носители кому-либо;

вводить в ОТСС персональные данные под диктовку или с микрофона;

осуществлять попытки несанкционированного доступа к ресурсам ИСПДн, проводить или участвовать в сетевых атаках и сетевом взломе;

производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов;

закрывать доступ к информации паролями без согласования с администратором информационной безопасности;

оставлять без личного присмотра на рабочем месте или где бы то ни было персональное устройство идентификации, машинные (съемные) носители и распечатки, содержащие защищаемую информацию;

9. Пользователь обязан обеспечить:

сохранность оборудования и физической целостности системных блоков компьютеров;

блокирование своей учетной записи в случае кратковременного оставления АРМ (нажатием клавиш Windows+L);

обязательное выключение компьютера после завершения работы;

10. Права пользователя:

участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС, если данное нарушение произошло под его идентификационными данными;

своевременно получать доступ к информационным ресурсам ИС, необходимым ему для выполнения своих должностных обязанностей;

требовать от администратора информационной безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

11. Ответственность:

Пользователь несет персональную ответственность за соблюдение установленных требований во время работы. Пользователи, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по Закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно распорядительными документами;

пользователь отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники;

нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей или ИСПДн в целом, может повлечь ответственность в соответствии с действующим законодательством.

**3. Работа с файлами документов, внесение корректировок, уничтожение, хранение документов**

| **№**  **п.п.** | **Этап** | **Описание этапа** |
| --- | --- | --- |
| **12. Подготовка к обработке информации** | | |
| 1 | Получение допуска к работе | Допуск работников органа власти к ИС осуществляется в соответствии с Списком лиц, допущенных к самостоятельной работе на ИС и разрешительной системе допуска к информационным ресурсам и техническим средствам.  Для работы в ИС каждый пользователь должен получить соответствующий допуск.  Права по доступу к информационным ресурсам должны быть определенны утверждённой Разрешительной системой допуска к данной ИС |
| 2 | Получение исходной информации для обработки в системе | Исходная информация, обработка которой осуществляется в системе, может находиться на учтённых сменных носителях информации (съемных жестких дисках, дискетах, компакт-дисках, бумажных носителях) |
| 3 | Вход пользователя в систему | Авторизация пользователя осуществляется средствами защиты информации по имени и с использованием его персонального пароля длиной не менее 6 символов |
| **13. Обработка информации** | | |
| 1 | Регистрация времени начала работы | Осуществляется средствами защиты информации |
| 2 | Ввод обрабатываемых исходных данных в систему | Ввод в систему обрабатываемой информации производится вручную с клавиатуры или путем считывания в электронном виде с дискет или компакт-дисков. |
| 3 | Обработка текстовой информации | Пользователь обязан принять меры по исключению возможности просмотра обрабатываемой информации с экрана монитора и с бумажных носителей (в том числе распечатываемых материалов) лицами, не допущенными к обрабатываемой информации. |
| 4 | Временное хранение обрабатываемой информации между сеансами работы пользователя в системе | Хранение обрабатываемой информации, между сеансами работы в системе, пользователь осуществляет в каталогах на жестком диске ПЭВМ, выделенных в системе для соответствующих видов обрабатываемой информации. Контроль доступа к ним осуществляется соответствующими средствами защиты информации |
| **14. Сохранение результатов обработки информации** | | |
| 1 | Распечатка документов | Распечатка документов (данных) производится на принтере, входящем в состав ОТСС объекта, средствами защиты информации может осуществляться учет распечатанных документов. |
| 2 | Сохранение окончательных результатов работы | Готовые данные в электронном виде содержатся на жёстком диске ОТСС ИС, регистрация и контроль доступа к ним осуществляется средствами защиты информации. |
| 3 | Передача носителей информации и распечатанных документов | В соответствии с требованиями организационно-распорядительных документов Аппарата Губернатора и Правительства автономного округа |
| 4 | Очистка остаточной (удаленной) информации | Гарантированная очистка удаляемой с накопителей информации (без возможности ее восстановления) осуществляется средствами защиты информации |
| 5 | Регистрация времени работы и действий пользователя в системе | Осуществляется средствами защиты информации |
| 6 | Завершение работы | После окончания работы с ИС, сотрудник обязан на своем рабочем месте завершить работу всех программ, входящих в состав специализированного программного обеспечения и выключить компьютер (перегрузить). В случаи необходимости оставить свое рабочее место на непродолжительное время пользователь обязан его заблокировать (дальнейшая работа может быть продолжена пользователем только после ввода его логина и пароля).  После окончания рабочего дня необходимо закрыть окна и форточки, выключать электроприборы, запереть дверь и включить охранную сигнализацию, при наличии таковой |

15. Подготовка, отправка, размножение, копирование, учет, распечатка необходимого числа экземпляров подготовленных документов, содержащих информацию ограниченного доступа.

Печать производится на принтере, входящем в состав ИС.

Размножение (копирование) документов, содержащих информацию ограниченного доступа, осуществляется только на МФУ, входящих в состав аттестованного СВТ или на аттестованном средстве изготовления и размножения документов (копир) органа власти.

Подготовка, учет, отправка, документов содержащих информацию ограниченного доступа осуществляется в соответствии с требованиями раздела XI «Порядок обращения с конфиденциальной информацией» постановления Губернатора Ханты-Мансийского автономного округа – Югры от 30 декабря 2012 года № 176 «Об Инструкции по делопроизводству в государственных органах Ханты-Мансийского автономного округа – Югры и исполнительных органах государственной власти Ханты-Мансийского автономного округа – Югры» (с изменениями, внесенными постановлением Губернатора автономного округа от 16.05.2014 № 57).