АДМИНИСТРАЦИЯ ГОРОДА ЮГОРСКА

Ханты-Мансийского автономного округа - Югры

РАСПОРЯЖЕНИЕ

от 14 декабря 2017 года №754

Об утверждении организационно-
распорядительных документов

В соответствии с постановлением Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», пунктом 1.4 протокола от 29.05.2017 № 3/17 заседания Совета по вопросам технической защиты информации в Ханты-Мансийском автономном округе-Югре утвердить следующие организационно-распорядительные документы, разработанных в области обеспечения безопасности информации:

1. Инструкцию для работников, эксплуатирующих информационную систему обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные в органах и структурных подразделениях администрации города Югорска (приложение 1);

2. Перечень функций должностного лица, ответственного за руководство работами по защите информации в органах и структурных подразделениях администрации города Югорска (приложение 2);

3. Инструкцию для должностного лица, ответственного за реализацию мероприятий по защите информации в органах и структурных подразделениях администрации города Югорска (приложение 3);

4. Инструкцию для должностного лица, ответственного за организацию обработки персональных данных в органах и структурных подразделениях администрации города Югорска (приложение 4);

5. Инструкцию для администратора информационной безопасности в органах и структурных подразделениях администрации города Югорска (приложение 5).

Исполняющий обязанности
главы города Югорска С.Д. Голин

Приложение 1
к распоряжению
администрации города Югорска
от 14 декабря 2017 года **№** 754

Инструкция для работников, эксплуатирующих информационную систему обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные в органах и структурных подразделениях администрации города Югорска

1. Общие положения

1. Настоящий документ определяет основные обязанности, права и ответственность работников (далее - Пользователь), эксплуатирующих информационную систему обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные (далее - информационная система (ИС)) в органах и структурных подразделениях администрации города Югорска (далее - Администрация).

2. Пользователем ИС является работник администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информая^ии и имеющий доступ к аппаратным средствам, программному обеспечению и данным . J, 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:

1) 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;

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

3) обеспечение необходимого уровня безопасности носителей КИ;

4) обеспечение безопасности конфиденциальной информации при её копировании, размножении;

5) 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, несёт персональную ответственность за свои действия и обязан:

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

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

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

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

5) выполнять требования «Инструкции по организации антивирусной защиты»;

6) 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;

7) 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;

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

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

10) при работе в ИС выполнять только служебные задания;

11) при отсутствии необходимости работы выключить (блокировать) компьютер;

12) при работе в ИС использовать только учтённые съёмные 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.), незамедлительно удалять информацию с носителей;

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

14) немедленно выполнять предписания администратора безопасности в части обеспечения безопасности информации;

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

16) соблюдать установленный режим разграничения доступа к информационным ресурсам;

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

18) 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:

1) 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;

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

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

4) работать с неучтёнными машинными (съёмными) носителями информации;

5) отключать (блокировать) средства защиты информации;

6) производить какие-либо изменения в размещении технических средств;

7) 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;

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

9) хранить на учтённых носителях программы и данные, не относящиеся к рабочей информации;

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

11) передавать свои учтённые носители кому-либо;

12) вводить в ОТСС персональные данные под диктовку или с микрофона;

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

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

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

16) оставлять без личного присмотра на рабочем месте или где бы то ни *I* ..о персональное устройство идентификации, машинные (съёмные) носители и распечатки, содержащие защищаемую информацию.

9. Пользователь обязан обеспечить:

1) сохранность оборудования и физической целостности системных блоков компьютеров;

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

3) обязательное выключение компьютера после завершения работы.

10. Пользователь имеет право:

1) 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;

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

3) требовать от администратора информационной безопасности см<^ i идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

11. Ответственность:

1) пользователь несёт 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;

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

Нарушение данной инструкции, повлёкшее 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 администрации 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 определены 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 (съёмных жёстких 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 путём 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 жёстком 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 учёт распечатанных документов.

№ п.п.	Этап	Описание этапа
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
4	Очистка остаточной (удалённой) информации	Гарантированная очистка удаляемой с накопителей информации (без возможности её 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 сво£м рабочем месте завершить работу всех программ, входягц. .. в состав специализированного программного обеспечения и выключить компьютер (перегрузить). В случаи необходимости оставить своё 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, учёт, 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 э на аттестованном средстве изготовления и размножения документов (копир).

Приложение 2

к распоряжению
администрации города Югорска
от 14 декабря 2017 года **№** 754

Перечень функций
должностного лица, ответственного за руководство работами по защите информации в органах и структурных подразделениях администрации города Югорска

Лицо, ответственное за руководство работами по защите информации в органах и структурных подразделениях администрации города Югорска, выполняет следующие основные функции:

1) руководство и координация деятельности по обеспечению безопасности информации в соответствии с требованиями законодательством Российской Федерации, нормативных правовых актов Президента и Правительства Российской Федерации, руководящих и методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и ФСБ России;

2) контроль вьшолнения работ по информационной безопасности;

3) определение возможности распространения (передачи) персональных данных и иной конфиденциальной информации;

4) согласование назначения лица, ответственного за организацию обработки персональных данных;

5) согласование назначения лиц, ответственных за контроль вьшолнения требований по обработке персональных данных;

6) согласование назначения администратора информационной безопасности информационных систем (далее - ИС);

7) координация вопросов обучения, повышения квалификации в области обеспечения информационной безопасности в учебных заведениях, программы которых согласованы ФСТЭК России;

8) представление на утверждение главе города Югорска перечня лиц, доступ которых к конфиденциальной информации, обрабатываемой в ИС, необходим для вьшолнения служебных обязанностей;

9) контроль функционирования системы защиты информации в органах и структурных подразделениях администрации города Югорска;

10) контроль соответствия реального состава пользователей матрице доступа;

11) контроль лиц, допущенных к работе с конфиденциальной информацией в ИС;

12) согласование документов, определяющих построение, внедрение, модернизацию системы защиты информации в ИС;

13) контроль за уровнем безопасности информации в органах и структурных подразделениях администрации города Югорска;

14) проведение служебных проверок по фактам несоблюдения условий, которые могут привести к нарушению конфиденциальности информации или другим нарушениям, приводящим к снижению уровня защищённости информации;

15) координация и руководство работой постоянно действующей технической комиссии (ПДТК) по защите информации.

Приложение 3
к распоряжению
администрации города Югорска
от 14 декабря 2017 года **№** 754

Инструкция для должностного лица,
ответственного за реализацию мероприятий по защите информации
в органах и структурных подразделениях администрации города Югорска

1. Лицо, ответственное за реализацию мероприятий по защите информации в органах и структурных подразделениях администрации города Югорска, выполняет следующие функции:

1) планирование работ по защите информации, контроль выполнения запланированных мероприятий, подготовку и представление отчёта о мероприятиях по защите информации в Управление защиты информации и специальной документальной связи Аппарата Губернатора автономного округа;

2) определение возможностей по получению охраняемых сведений техническими средствами разведки иностранных государств и криминальных структур;

3) определение технических каналов утечки информации, возможностей несанкционированного доступа к информационным ресурсам и процессам и воздействия на них с целью разрушения (уничтожения) или искажения;

4) подготовка предложений по классификации автоматизированных систем (далее - АС) по уровню их защиты от несанкционированного доступа к информационным ресурсам и процессам;

5) разработка предложений по организационно-техническим мероприятиям защиты информации на объектах информатизации;

6) организация подготовки объектов информатизации, обрабатывающих информацию ограниченного доступа к аттестации, организация и участие в разработке необходимой документации, в том числе технических паспортов на объекты информатизации;

7) формирование предложений в план закупки и внедрения новых технических средств в области защиты информации, внесение предложений по финансированию работ, связанных с обеспечением защиты информации, обрабатываемой на объектах информатизации, исходя из требований;

8) организация аттестации объектов информатизации по требованиям безопасности информации;

9) разработка предложений по организации и совершенствованию системы защиты информации;

10) разработка руководящих и организационных документов по защите информации;

11) организация и проведение периодического контроля эффективности проводимых мероприятий и принимаемых мер по защите информации, учёт и анализ результатов контроля;

12) организация в установленном порядке расследований причин и условий появления нарушений в области защиты информации и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений;

13) организация и проведение занятий с сотрудниками органов и структурных подразделений администрации города Югорска по вопросам защиты информации;

14) учёт лиц, допущенных к работе с конфиденциальной информацией в информационных системах (далее - ИС);

15) определение угроз безопасности информации, формирование на их основе модели угроз и модели нарушителя безопасности информации в ИС;

16) разработка на основе модели угроз системы защиты информации ИС, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты информации, предусмотренных для соответствующего класса информационных систем;

17) контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

18) незамедлительное информирование главы города Югорска (лица, ответственного за руководство работами по защите информации) об имевших место попытках несанкционированного доступа к конфиденциальной информации, а также разработка мер по их недопущению;

19) обеспечение соблюдения требований по обеспечению информационной безопасности при проведении технического обслуживания и ремонтных работ в информационной системе;

20) проведение инструктажа работников органа власти по правилам работы с используемыми аппаратно-программными средствами защиты информации;

21) повседневный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования;

22) предоставление в отдел технической защиты информации Управления специальных мероприятий Аппарата Губернатора автономного округа необходимой информации в части возложенных на него полномочий и обязанностей в пределах своей компетенции.

2. Лицо, ответственное за реализацию мероприятий по защите информации в органах и структурных подразделениях администрации города Югорска, имеет право:

1) выходить с предложениями к руководству по совершенствованию системы защиты информации в органах и структурных подразделениях администрации города Югорска и привлечению к проведению работ по запщте информации на договорной основе предприятий и организаций, имеющих лицензии на соответствующий вид деятельности;

2) контролировать выполнение требований по защите информации при эксплуатации объектов информатизации;

3) вносить предложения руководству о прекращении обработки информации на объектах информатизации при выявлении нарушений, приводящих к утечке информации.

Приложение 4
к распоряжению
администрации города Югорска
от 14 декабря 2017 года **№** 754

Инструкция для должностного лица,
ответственного за организацию обработки персональных данных
в органах и структурных подразделениях администрации города Югорска

1. Лицо, ответственное за организацию обработки персональных данных в органах и структурных подразделениях администрации города Югорска, выполняет следующие функции:

1) подготовка и предоставление на утверждение главе города Югорска перечня должностей работников, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным;

2) участие в определении полномочий пользователей информационных систем персональных данных (далее - ИСПДн) (оформление разрешительной системы доступа), минимально необходимых им для выполнения служебных обязанностей;

3) контроль выполнения мероприятий по защите информации в ИСПДн;

4) внесение предложений по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последсто. *i* нарушений, приводящих к снижению уровня защищённости персональных данных в следствии неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных (далее - ПДн);

5) проведение занятий и инструктажей с работниками органов и структурных подразделений администрации города Югорска о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности ПДн;

6) контроль соблюдения работниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными, машинными носителями информации;

7) внутренний контроль за соблюдением работниками требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

8) проведение разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привес ^ к снижению уровня защищённости персональных данных;

9) представление интересов администрации города Югорска при проверках надзорных органов в сфере обработки персональных данных;

10) вьшолнение иных мероприятий, требуемых нормативными документами по защите персональных данных.

2. Действия при обнаружении попыток несанкционированного доступа.

2.1. К попыткам несанкционированного доступа относятся:

1) сеансы работы с ПДн незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

2) действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

2.2. При выявлении факта несанкционированного доступа лицо, выявившее факт несанкционированного доступа (пользователи, ответственный за организацию обработки ПДн, лицо, ответственное за вьшолнение требований по обработке ПДн в структурных подразделениях органа власти, администратор информационной безопасности) обязаны:

1) законными способами прекратить несанкционированный доступ к ПДн;

2) известить администратора информационной безопасности ИСПДн о факте несанкционированного доступа;

3) известить руководителя структурного подразделения, в котором работает пользователь, от имени учётной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4) известить руководство администрации города Югорска.

2.3. Лицо, ответственное за руководство работами по защите информации в органе власти, организует разбирательство по факту несанкционированного доступа.

2.4. По результатам разбирательства лицо, ответственное за организацию обработки ПДн докладывает заместителю руководителя лицу, ответственному за руководство работами по защите информации в органе власти служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях.

3. Ответственный за организацию обработки персональных данных в органах и структурных подразделениях администрации города Югорска имеют право:

1) требовать от работников выполнения федерального закона «О персональных данных» и принятых в соответствии с ним нормативными правовыми актами, а также локальных нормативно-правовых актов в части работы с персональными данными;

2) блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн;

3) проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных;

4) привлекать к реализации мер, направленных на выполнение требований законодательства о персональных данных, иных работников с возложением на них соответствующих обязанностей и закреплением ответственности;

5) иметь доступ к информации, касающейся обработки персональных данных в соответствующем структурном подразделении органа власти и включающей:

- цели обработки персональных данных;
- категории обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовые основания обработки персональных данных;
- перечень действий с персональными данными;
- дату начала обработки персональных данных;
- срок или условия прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

4. Ответственный за организацию обработки персональных данных в органах и структурных подразделениях администрации города Югорска несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обработке и обеспечению безопасности персональных данных. Данное должностное лицо при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 5
к распоряжению
администрации города Югорска
от 14 декабря 2017 года **№** 754

Инструкция для администратора информационной безопасности в органах и структурных подразделениях администрации города Югорска

1. Администратор информационной безопасности (далее - администратор ИБ) осуществляет контроль выполнения требований организационных и технических мероприятий по обеспечению безопасности информации в информационных системах (далее - ИС).

2. Администратор ИБ 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.

3. Основными задачами администратора ИБ являются:

1) 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 администрации города Югорска;

2) обеспечение в ИС необходимого уровня безопасности обработки, хранения и переда[1] КИ;

3) обеспечение необходимого уровня безопасности носителей КИ;

4) обеспечение безопасности конфиденциальной информации при её копировании, размножении;

5) резервное копирование, восстановление информации.

4. Обязанности администратора информационной безопасности:

1) знать нормативно-методические документы и муниципальные правовые актов в области безопасности информации;

2) знать состав основных технических средств и систем (далее - ОТСС) ИС и контролировать их соответствие техническому паспорту на ИС. Вести учёт изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения);

3) контролировать процесс управления (заведения, активации, блокирования, уничтожения) учётными записями пользователей ИС;

4) проверять соответствие прав доступа пользователей к объектам доступа ИС в соответствии с задачами, решаемыми пользователями в ИС и взаимодействующими с ней *W^* и Разрешительной системой доступа к ИС:

5) контролировать назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС;

6) проверять отсутствие в ИС учётных записей уволенных (отстранённых) сотрудников;

7) оповещать администратора, осуществляющего управление учётными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

8) проверять своевременность удаления временных учётных записей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИС;

9) контролировать неизменность настроек средств защиты информации, настройки средств защиты информации должны неизменно выполнять:

10) препятствовать передаче защищаемой информации через сеть Интернет и (или) другие информационно-телекоммуникационные сети международного информационного обмена по незащищённым линиям связи;

11) ограничивать доступ к ИС на 10 минут при 3 неудачных попытках входа в ИС;

12) запрещать доступ к ИС до прохождения процедур аутентификации и идентификации;

13) запрещать удалённый доступ к ИС;

14) контролировать запрет использования в ИС технологий беспроводного доступа и мобильных технических средств;

15) контролировать отсутствие доступа к ИС со стороны пользователей информационных систем сторонних организаций;

16) контролировать установку на АРМ ИС программного обеспечения (далее - ПО), не связанного с задачами, решаемыми пользователями в ИС;

17) обеспечивать учёт съёмных машинных носителей конфиденциальной информации (далее - СМНКИ);

18) обеспечивать уничтожение (стирание) защищаемой информации с машинных носителей АРМ ИС, при их передаче в сторонние организации для ремонта или утилизации, либо контролировать процесс уничтожения (стирания). Уничтожение защищаемой информации должно исключать возможность восстановления защищаемой информации.

19) контролировать регистрацию в ИС следующих событий безопасности:

- входа (выхода), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы (дата (время) входа/выхода в систему (из системы) или загрузки/останова операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа);

- подключения машинных носителей информации и вывода информации на носители информации (дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации);

- запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации (дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный));

- попыток доступа программных средств к защищаемым объектам доступа (дата и время попытки доступа к защищаемому файлу с указанием её результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого файла (логическое имя, тип));

- попыток удалённого доступа (дату и время попытки удалённого доступа с указанием её результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удалённого доступа к информационной системе).

20) контролировать права на доступ к информации о событиях безопасности: доступ должен предоставляться исключительно администратору информационной безопасности, а также системному администратору ИС, обеспечивающим функционирование ИС.

21) обеспечивать постоянный контроль за выполнением пользователями ИС установленного комплекса мероприятий по обеспечению безопасности информации и соблюдения действующего законодательства в области информационной безопасности, а также инструкции пользователя и других организационно-распорядительных документов в части обеспечения безопасности информации;

22) требовать от пользователей ИС и выполнять самому требования «Инструкции по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств ИС»;

23) контролировать порядок учёта, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов;

24) контролировать использование пользователями только учтённых съёмных носителей. После того как цель переноса информации достигнута (передача третьим лицам и т.п.), информация незамедлительно должна быть удалена с носителей;

25) контролировать настройки ОС и СЗИ АРМ пользователей;

26) проводить инструктаж пользователей по правилам работы с используемыми средствами и системами зашиты информации;

27) устанавливать права доступа пользователей к информационным и техническим ресурсам ИС в соответствии с принятой и утверждённой разрешительной системой доступа;

28) следить за изменением программной среды ИС и полномочиями пользователей;

29) хранить дистрибутивы СЗИ, производить при необходимости восстановление программной среды СЗИ или настройки защитных механизмов операционной системы и привилегий пользователей по доступу к ресурсам ИС. При необходимости для данных мероприятий привлекать других технических специалистов отдела ЗИ;

30) фиксировать и пресекать невыполнение пользователями ИС требований или норм нормативно-методических документов в области безопасности информации и организационно-распорядительных документов в информационной сфере, а также создания пользователями возможностей утечки информации;

31) при получении информации о фактах нарушения политики и правил безопасности, а также попыток использования внешними нарушителями атак, в том числе с использованием методов социальной инженерии — немедленно докладывать ответственному за организацию обработки персональных данных, инициировать проведение служебной проверки (при нарушениях со стороны ответственного за организацию обработки персональных данных докладывать необходимо непосредственно вышестоящему руководству), регистрировать в журнале учёта инцидентов ИБ;

32) не реже 1 раза в квартал просматривать журналы учёта и регистрации событий СЗИ (в соответствии с инструкцией по использованию программных и аппаратных средств защиты информации, операционной системы на предмет выявления подключения неучтённых носителей, попыток НСД и т.п.;

33) требовать от пользователей ИС и выполнять самому требования инструктора о пропускном и внутриобъектовом режимах в зданиях администрации города Югорска;

34) контролировать отсутствие в составе ПО АРМ, входящих в ИС, средств разработки и отладки программ;

35) реагировать на поступление в ИС спама (в случае присутствия данной информации в журналах событий межсетевого экрана) путём блокирования атакующего хоста;

36) выполнять мероприятия по периодическому резервному копированию защищаемой информации в соответствии с «Инструкцией по резервному копированию и восстановлению данных»;

37) знать эксплуатационную документацию на применяемые СЗИ. Устанавливать и эксплуатировать СЗИ в соответствии с документацией;

38) хранить документацию и дистрибутивы СЗИ в соответствии с техническими условиями. Компакт-диск с программным обеспечением системы должен упаковываться согласно требованиям, предусмотренным для оптических носителей;

39) поддерживать настройки СЗИ, соответствующие требованиям нормативных документов по безопасности информации и протоколу аттестационных испытаний, при этом система должна реализовывать в совокупности на каждой АРМ ИС функции необходимые для выполнения требований по защите от несанкционированного доступа (далее - НСД) для ИС;

40) контролировать срок действия сертификатов соответствия на СЗИ и обеспечить их продление в соответствии с порядком продления, приведённым ниже.

5. Администратор ИБ оказывает методическую помощь и контролирует выполнение руководителем структурного подразделения, эксплуатирующего ИС, следующих действий:

1) при смене пользователя руководитель структурного подразделения, эксплуатирующего ИС, инициирует внесение изменений в список работников, допущенных к работе в данной ИС и в разрешительную систему доступа;

2) при исключении пользователя ИС из «Перечня лиц, имеющих доступ к самостоятельной работе в ИС» руководителем подразделения, эксплуатирующего ИС, принимаются меры по исключению возможности нарушения данным пользователем характеристик безопасности информации ИС.

Администратору информационной безопасности необходимо до момента доведения до сотрудника информации о прекращении его работы в ИС, лишить сотрудника возможности доступа к защищаемой информации.

6. Администратору ИБ запрещается:

1) фиксировать учётные данные пользователя (пароли, идентификаторы, ключи и др.) на твёрдых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя;

2) раскрывать информацию об организации системы защиты КИ в органах и структурных подразделениях администрации города Югорска и любую информацию, которая

может создать предпосылки для возникновения канала утечки информации или создания угрозы безопасности информации.

7. Администратор ИБ имеет право:

1) требовать от пользователей ИС соблюдения установленных технологий обработки информации, выполнения нормативно-методических документов в области безопасности информации и организационно-распорядительных документов на ИС;

2) давать своему непосредственному начальнику предложения по совершенствованию мер защиты в ИС;

3) инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

8. Администратор ИБ несёт ответственность в соответствии с действующим законодательством за разглашение сведений ограниченного распространения, ставших известными ему по роду деятельности.

9. На администратора ИБ возлагается ответственность за защиту ИС от несанкционированного доступа к информации и за неукоснительное соблюдение положений настоящей инструкции.