МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ

КИНДАЛЬСКОЕ СЕЛЬСКОЕ ПОСЕЛЕНИЕ

КАРГАСОКСКОГО РАЙОНА ТОМСКОЙ ОБЛАСТИ

МУНИЦИПАЛЬНОЕ КАЗЁННОЕ УЧРЕЖДЕНИЕ

«АДМИНИСТРАЦИЯ КИНДАЛЬСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ»

РАСПОРЯЖЕНИЕ

02.04.2014 № 12

с. Киндал

Об утверждении инструкции по

защите ПД (персональных данных)

В целях реализации требований Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных»

1.Утвердить следующие инструкции:

1. Инструкция администратора ИСПДн. Приложение 1.

2. Инструкция по обеспечению мер пожарной безопасности. Приложение 2.

3. Инструкция администратора по информационной безопасности. Приложение 3.

4. Инструкция пользователя информационной системы персональных данных. Приложение 4.

5. Инструкция пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций. Приложение 5.

2.Настоящее распоряжение обнародовать (опубликовать) на сайте в информационной сети интернет Киндальского сельского поселения.

Глава Киндальского

сельского поселения Волков В.В.

Приложение 1

«УТВЕРЖДЕНО»

Распоряжением Администрации Киндальского сельского поселения

№ 02.04.2014 № 12

Инструкция

администратора ИСПДн

1. Общие положения

1.1. Администратор ИСПДн (далее - Администратор) назначается распоряжением Главы Администрации Киндальского сельского поселения (далее - руководителя Оператора), на основании Положения о разграничении прав доступа к обрабатываемым персональным данным.

1.2. Администратор подчиняется руководителю Оператора.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, Концепцией и Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Оператора.

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

1.5. Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

2. Функции

2.1. Администратор обеспечивает устойчивую работоспособность элементов ИСПДн, средств ее защиты при обработке персональных данных, локальной вычислительной сети.

3. Должностные обязанности

3.1. Администратор обязан:

3.2. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

3.3. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);

- аппаратных средств;

- аппаратных и программных средств защиты.

3.4. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

3.5. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

3.6. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

3.7. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.8. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.

3.9. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.

3.10. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

3.11. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

3.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт.

Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

3.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

3.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий

4. Права и полномочия

4.1. Администратор имеет право:

4.2. Требовать от сотрудников Оператора соблюдения установленного комплекса мероприятий по обеспечению безопасности информации

4.3. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследованиях фактов (попыток) несанкционированного доступа;

4.4. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

5. Ответственность

5.1. Администратору необходимо отвечать за свои действия (бездействия) в рамках зафиксированных в п.п 3, 4 настоящей инструкции обязанностей, прав и полномочий.

5.2. Администратор несет дисциплинарную, материальную, гражданско-правовую, административную и уголовную ответственность в порядке, предусмотренном законодательством.

Приложение 3

«УТВЕРЖДЕНО»

Распоряжением Администрации Киндальского сельского поселения

№ 02.04.2014 № 12

Инструкция

администратора по информационной безопасности

Настоящая инструкция определяет общие функции, права и обязанности администратора безопасности по вопросам обеспечения информационной безопасности при подготовке и обработки персональных данных на ПЭВМ, входящих в состав информационной системы персональных данных (далее по тексту- ИСПДн).

Администратор безопасности информации назначается из числа сотрудников Администрации Киндальского сельского поселения (далее – Оператора) и обеспечивает правильное использование и функционирование установленных средств защиты информации (далее по тексту – СЗИ) от несанкционированного доступа (далее по тексту – НСД).

Администратор безопасности информации имеет все права администратора СЗИ от НСД.

Настоящая Инструкция разработана на основании действующих нормативных документов по защите персональных данных.

1. Основные функции администратора безопасности

1.1. Контроль за выполнением требований действующих нормативных и руководящих документов по защите персональных данных, при проведении работ на ПЭВМ.

1.2. Работа с учетными записями пользователей ИСПДн (удаление, регистрация новых пользователей), их правильная настройка и разграничение прав доступа пользователей к защищаемым ресурсам ИСПДн согласно разрешительной системе доступа.

1.3. Своевременная корректировка разрешительной системы доступа:

- изменение списка постоянных пользователей ИСПДн (ввод или удаление пользователя из ИСПДн);

- изменение прав доступа к защищаемым программным ресурсам или портам ввода-вывода ИСПДн.

1.4. Корректировка разрешительной системы доступа осуществляется на основании служебной записки пользователя, согласованной с ответственным за эксплуатацию объекта и утвержденной Главой Администрации Киндальского сельского поселения.

1.5. Контроль доступа пользователей к работе на ПЭВМ (в соответствии со списком допущенных сотрудников), выдача внешних носителей информации и соблюдения пользователями требований нормативных  и руководящих документов (в том числе путем просмотра системного журнала).

1.6. Контроль за ежеквартальным проведением пользователями ИСПДн смены их личных паролей для доступа к ПЭВМ.

1.7. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе на ПЭВМ, в том числе и в части периодического контроля за печатью файлов пользователей на принтере и соблюдением установленных правил и параметров регистрации и учета документов, бумажных и машинных носителей информации.

1.8. Сопровождение подсистемы обеспечения целостности информации на ПЭВМ:

- периодический контроль за отсутствием на жестком магнитном диске ПЭВМ остаточной информации по окончании работы пользователей;

- поддержание установленного порядка и правил антивирусной защиты информации, обрабатываемой на ПЭВМ;

- контроль за соблюдением пользователями инструкции по антивирусному контролю. Программирование, выдача и учет выдачи пользователям электронных ключей от СЗИ НСД (при их наличии).

1.9. Контроль за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусе ПЭВМ и устройств.

1.10. Контроль за вскрытием и ремонтом (модернизацией) ПЭВМ, недопущением доступа посторонних лиц к конфиденциальной информации во время вскрытия, ремонта, модернизации ПЭВМ или устройств, последующим опечатыванием ПЭВМ (устройств), составлением соответствующих актов.

1.11. Контроль срока действия сертификатов соответствия ФСТЭК России на средства защиты от несанкционированного доступа, установленных на ИСПДн.

2. Права Администратора безопасности

2.1 Администратор безопасности имеет право:

2.2. Требовать от сотрудников Оператора соблюдения установленной технологии обработки конфиденциальной информации и исполнения настоящей Инструкции.

2.2. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследованиях фактов (попыток) несанкционированного доступа;

2.3. Требовать от пользователей прекращения обработки информации в ИСПДн в случае:

- нарушения установленного порядка работ;

- нарушения работоспособности средств и систем защиты информации или окончания срока действия сертификатов соответствия ФСБ России или ФСТЭК России;

- получения информации о возможном проведении технической разведки в отношении ИСПДн.

3. Обязанности администратора безопасности

3.1. Администратор безопасности обязан:

3.2. Обеспечивать правильное функционирование и поддерживать работоспособность средств и СЗИ от НСД в пределах возложенных на него функций;

3.3.В случае отказа СЗИ от НСД принимать меры по их восстановлению;

3.4. Проводить инструктаж пользователей по правилам работы на ПЭВМ, с установленной СЗИ от НСД;

3.5. Немедленно докладывать (по подчиненности) ответственному за эксплуатацию ИСПДн, Главе Администрации Киндальского сельского поселения или лицу, исполняющему его обязанности, о фактах и попытках несанкционированного доступа к персональным данным, о неправомерных действиях пользователей или иных лиц, приводящих к нарушению требований по защите информации, а также об иных нарушениях требований информационной безопасности ИСПДн.

3.6.Вносить изменения в документацию ИСПДн в соответствии с требованиями нормативных документов в части, касающейся СЗИ от НСД;

3.7. Проводить работу по выявлению возможных каналов утечки конфиденциальной информации, вести их учёт и принимать меры к их устранению;

3.8. Осуществлять не реже одного раза в неделю обновление антивирусных баз на ПЭВМ в ИСПДн;

3.9. Контролировать целостность (неизменность, сохранность) программного обеспечения, разрешительной системы доступа, а при обнаружении фактов изменения проверяемых параметров немедленно докладывать по подчинённости;

3.10. Вводить полномочия работников в разрешительную систему доступа, обеспечивать их своевременную корректировку;

3.11. Регистрировать факты выдачи внешних носителей в журнале учета выдачи внешних носителей.

3.12. Требовать от пользователей прекращения обработки информации ИСПДн при появлении информации о возможном проведении технической разведки в отношении ИСПДн.

3.13. Заблокировать учетные записи пользователей на ПЭВМ в случае окончания срока действия сертификата соответствия ФСТЭК России, ФСБ России на любое СЗИ, из используемых в ИСПДн, до момента его продления. В случае не продления сертификата соответствия ФСТЭК России на СЗИ он обязан поставить в известность орган по аттестации, проводивший аттестацию ИСПДн, для принятия совместного решения.

3.14. Контролировать действия пользователей по правильности затирания информации на внешних накопителях информации.

Приложение 2

«УТВЕРЖДЕНО»

Распоряжением Администрации Киндальского сельского поселения

№ 02.04.2014 № 12

Инструкция

по обеспечению мер пожарной безопасности

1. Общие положения

1.1. Инструкция по обеспечению мер пожарной безопасности в административных зданиях (далее – Инструкция) разработана на основе Правил пожарной безопасности в Российской Федерации (ППБ 01-03), утвержденных приказом Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий от 18 июня 2003г. N 313 и устанавливает обязательные для исполнения требования пожарной безопасности в административных зданиях по обеспечению в здании пожарной безопасности, предупреждению возникновения чрезвычайных ситуаций, участию в организации тушения пожаров и ликвидации их последствий.

1.2. Требования Инструкции направлены на осуществление в зданиях противопожарных мероприятий, разработанных с учетом насыщенности зданий инженерным оборудованием, техническими средствами, служебными документами и материальными ценностями.

1.3. Ответственность за соблюдение правил пожарной безопасности в служебных помещениях и помещениях общего пользования возлагается на руководителей соответствующих структурных подразделений, а обязанности по контролю за соблюдением правил пожарной безопасности – на руководителей отделов.

1.4. Руководители структурных подразделений, сотрудники, допустившие нарушения Правил пожарной безопасности и Инструкции, несут ответственность в соответствии с законодательством Российской Федерации.

1.5. Общее руководство деятельностью структурных подразделений по обеспечению пожарной безопасности в здании осуществляется Главой Администрации Киндальского сельского поселения.

2. Эксплуатация служебных, подсобных и технических помещений

2.1. В здании запрещается:

1) хранить и применять в подвалах и подсобках легковоспламеняющиеся и горючие жидкости (далее – ЛВЖ и ГЖ), баллоны с газами, взрывопожароопасные вещества и материалы, кроме случаев, оговоренных в нормативных документах, а также хранить взрывоопасные вещества, ЛВЖ и ГЖ в кабинетах, служебных и иных помещениях, а также в письменных столах, шкафах, сейфах;

2) использовать чердаки и другие технические помещения для организации производственных участков, мастерских, а также для хранения в них оборудования, мебели и других предметов;

3) размещать кладовые и иные складские;

4) снимать предусмотренные проектом двери эвакуационных выходов коридоров, тамбуров , а также другие двери, препятствующие распространению опасных факторов пожара на путях эвакуации;

5) производить изменения объемно-планировочных решений, в результате которых ухудшаются условия безопасной эвакуации людей, ограничивается доступ к огнетушителям, пожарным кранам и другим средствам пожарной безопасности или уменьшается зона действия автоматических систем противопожарной защиты;

6) загромождать мебелью, оборудованием и другими предметами двери, переходы в смежные секции и выходы на наружные эвакуационные лестницы;

7) проводить уборку помещений и стирку одежды с применением бензина, керосина и других ЛВЖ и ГЖ, а также отогревать замерзшие трубы отопления паяльными лампами и другими способами с применением открытого огня;

8) устраивать в помещении кладовые (чуланы), а также хранить горючие материалы;

9) устанавливать дополнительные двери или изменять направление открывания дверей в общий коридор, если это будет препятствовать свободной эвакуации людей;

10) применять открытый огонь в помещениях, а также выполнять сварочные работы без согласования и без оформления наряда-допуска на производство работ;

11) производить перепланировку помещений без письменного согласия, изменять их функциональное назначение, устанавливать в них новое технологическое оборудование, электросети, а также устраивать в помещениях временные электропроводки;

12) курить в здании и на прилегающей территории, за исключением специально отведенных и оборудованных во внутреннем дворе мест для курения;

13) использовать для хозяйственных нужд рукава пожарных кранов, а также другие противопожарные средства и инвентарь;

14) оставлять открытыми двери чердачных помещений, технических сооружений.

3. Эксплуатация эвакуационных путей и выходов

3.1. При эксплуатации эвакуационных путей и выходов запрещается:

1) загромождать эвакуационные пути и выходы, в том числе проходы, коридоры, тамбуры, двери, эвакуационные люки, различными материалами, изделиями, оборудованием, производственными отходами, мусором и другими предметами, а также забивать двери эвакуационных выходов;

2) устраивать в тамбурах выходов сушилки и вешалки для одежды, гардеробы, а также постоянно или временно хранить в них инвентарь и материалы;

3) устраивать на путях эвакуации пороги (за исключением порогов в дверных проемах) устройства, препятствующие свободной эвакуации людей;

4) изменять направления открывания дверей по направлению выхода из здания, создавать препятствия свободному открыванию дверей на путях эвакуации из здания, за исключением дверей, открывание которых не регламентируется требованиями нормативных документов по пожарной безопасности;

5) заменять запоры на дверях эвакуационных выходов, обеспечивающие возможность свободного открывания запоров изнутри без ключа;

6) применять горючие материалы для отделки, облицовки и окраски стен и потолков, а также ступеней и лестничных площадок на путях эвакуации;

4. Эксплуатация электроустановок

4.1. При эксплуатации электроустановок запрещается:

1) использовать приемники электрической энергии в условиях, не соответствующих требованиям инструкций организаций-изготовителей, или приемники, имеющие неисправности, которые могут привести к пожару;

2) эксплуатировать электропровода и кабели с поврежденной или потерявшей защитные свойства изоляцией;

3) пользоваться поврежденными розетками, рубильниками, другими электроустановочными изделиями;

4) обертывать электролампы и светильники бумагой, тканью и другими горючими материалами, а также эксплуатировать светильники со снятыми колпаками (рассеивателями), предусмотренными их конструкциями;

5) пользоваться электроутюгами, электроплитками, электрочайниками и другими электронагревательными приборами, не имеющими исправных устройств тепловой защиты, без подставок из негорючих теплоизоляционных материалов, исключающих опасность возникновения пожара;

6) оставлять без присмотра включенными в электросеть радиоприемники, телевизоры, офисную технику, бытовые нагревательные и осветительные электроприборы, особенно электрочайники любого вида;

7) использовать одновременно, во избежание перегрузки электросети, электрочайники и другие бытовые нагревательные электроприборы (электрокамины, микроволновые печи и другие приборы);

8) эксплуатировать электронагревательные приборы при отсутствии или неисправности терморегуляторов, предусмотренных конструкцией;

9) применять нестандартные (самодельные) электронагревательные приборы, использовать некалиброванные плавкие вставки или другие самодельные аппараты защиты от перегрузок и коротких замыканий;

10) размещать (складировать) у электрощитов, электродвигателей и пусковой аппаратуры горючие вещества и материалы.

5. Полномочия руководителей

5.1. Руководитель предприятия, в целях пожарной безопасности здания/служебных помещений организует и осуществляет мероприятия в соответствии с полномочиями, предоставленными правовыми актами и Инструкцией.

5.2. Руководитель предприятия:

1) возлагает обязанности по контролю соблюдения правил пожарной безопасности и Инструкции на начальников отделов;

2) определяет минимальный объем документов и материальных ценностей, подлежащих эвакуации в случае возникновения угрозы их уничтожения или повреждения при пожаре;

3) организует проведение противопожарного инструктажа подчиненных служащих и работников;

4) обеспечивает ознакомление под роспись подчиненных служащих и работников с Инструкцией, а также с планом эвакуации.

5.3. Заместитель руководителя:

1) обеспечивает согласно установленным нормам первичными средствами пожаротушения (огнетушителями, пожарными кранами) с обозначением места их нахождения, а также стендами с планами эвакуации людей при возникновении пожара, автоматическими системами противопожарной защиты, громкоговорящей системой оповещения служащих и работников о пожаре, задымлении и других стихийных бедствиях;

2) организует и контролирует проведение мероприятий по пожарной безопасности технологических процессов, эксплуатации оборудования согласно техническим нормам и инструкциям по эксплуатации;

3) обеспечивает содержание прилегающей к зданию территории и помещений здания в состоянии, соответствующем противопожарным нормам и правилам, а также своевременную уборку мусора, горючих веществ и материалов;

4) организует проведение занятий по пожарно-техническому минимуму со всеми категориями лиц, подлежащих обучению;

5) организует и осуществляет контроль за выполнением правил пожарной безопасности структурными подразделениями, информирует о состоянии пожарной безопасности здания.

6. Соблюдение пожарной безопасности служащими и работниками

6.1. Служащие и работники в целях пожарной безопасности обязаны:

1) знать и соблюдать настоящую Инструкцию и ознакомиться с ней под роспись;

2) проходить вводный, первичный, повторный, внеплановый и целевой инструктажи по пожарной безопасности;

3) уметь пользоваться первичными средствами пожаротушения;

4) выполнять меры пожарной безопасности при пользовании электроприборами (компьютерами, кондиционерами, холодильниками, плитками, чайниками, утюгами и т.п.), газовыми приборами, предметами бытовой химии, а также при проведении работ с ЛВЖ, горючими материалами, другими опасными в пожарном отношении веществами;

5) знать план эвакуации из помещения и здания, на котором они занимают помещение;

6.2. Ответственный за противопожарное состояние помещения или последний уходящий из помещения по окончании рабочего дня обязан осмотреть помещение на предмет пожарной безопасности, выключить освещение, отключить от электросети оргтехнику и электроприборы, закрыть оконные форточки, запереть дверь.

7. Действия служащих и работников при получении информации о пожаре или его обнаружении

7.1. Служащие и работники при обнаружении пожара или признаков горения (запаха гари, задымления, повышенной температуры и т.п.) обязаны:

- сообщить о пожаре, по возможности указав точное место возгорания (адрес, этаж, номер служебного помещения), свою должность, фамилию и структурное подразделение, где работают: в районную пожарную охрану по телефону 01;

- своему руководителю;

- выполнять команды, поступившие от руководителя и по громкоговорящей системе оповещения;

- покинуть помещение в соответствии с планом эвакуации, взяв с собой комплект защиты органов дыхания (маску), оказывая помощь людям, имеющим затруднения при эвакуации из помещений.

7.2. Руководители структурных подразделений при получении информации о пожаре:

1) организуют и принимают предусмотренные планами эвакуации меры по эвакуации людей, документов, имущества;

2) немедленно оповещают подчиненных служащих и работников о возникшем пожаре, предлагают им срочно покинуть помещения в соответствии с планами эвакуации, осуществляют контроль за ее проведением;

3) дают указание лицам, ответственным за хранение и эвакуацию документов, об их выносе за пределы здания в соответствии с планами эвакуации, контролируют выполнение указания;

7.3. При возникновении пожара или задымления в здании эвакуация производится по зонам из всего здания согласно объявлениям автоматической системы оповещения о пожаре.

Приложение 4

«УТВЕРЖДЕНО»

Распоряжением Администрации Киндальского сельского поселения

№ 02.04.2014 № 12

Инструкция

пользователя информационной системы персональных данных

1. Общие положения

1.1. Пользователь информационной системы персональных данных (далее по тексту – ИСПДн) осуществляет обработку персональных данных в ИСПДн.

1.2. Пользователем является каждый сотрудник Администрации Киндальского сельского поселения (далее – Оператора), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Концепцией информационной безопасности, Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Оператора.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 4).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Оператора, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к лицу ответственному за обеспечение информационной безопасности ИСПДн.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.9. Пользователям запрещается:

- Разглашать защищаемую информацию третьим лицам.

- Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

- Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

- Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

- Отключать (блокировать) средства защиты информации.

- Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

2.11.Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3. Организация парольной защиты

3.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

- Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

- Пароль должен состоять не менее чем из 8 символов.

- В пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

- Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

- Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

- Запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

- Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранение пароля:

- Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

- своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

Приложение 5

«УТВЕРЖДЕНО»

Распоряжением Администрации Киндальского сельского поселения

№ 02.04.2014 № 12

Инструкция

пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций

1. Назначение и область действия

1.1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн Администрации Киндальского сельского поселения (далее - Оператора), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачей данной Инструкции является:

- определение мер защиты от прерывания;

- определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех пользователей Оператора, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;

- системы контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

2. Порядок реагирования на аварийную ситуацию

2.1. В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении 1.- "Источники угроз".

2.2. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Оператора (Администратор безопасности, Администратор и Оператор ИСПДн-сотрудник) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.3. Уровни реагирования на инцидент. При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

- Уровень 1 - Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

- Уровень 2 - Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

а) Отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;

- сбоя системы кондиционирования.

б) Отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:

- химического выброса в атмосферу;

- сбоев общественного транспорта;

- эпидемии;

- массового отравления персонала;

- сильного снегопада;

- шторма (ураганного ветра);

- сильных морозов.

- Уровень 3 - Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к работоспособности ИСПДн и средств защиты на сутки и более.

2.5. К катастрофам относятся следующие инциденты:

- пожар в здании;

- взрыв;

- просадка грунта с частичным обрушением здания;

- массовые беспорядки в непосредственной близости от Объекта.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

а) системы жизнеобеспечения, что включает:

- пожарные сигнализации и системы пожаротушения;

- системы вентиляции и кондиционирования;

- системы резервного питания.

б) системы обеспечения отказоустойчивости;

в) системы резервного копирования и хранения данных;

г) системы контроля физического доступа.

д) пожарные сигнализации и системы пожаротушения;

е) системы вентиляции и кондиционирования;

3.2. Все критичные помещения Оператора (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.3. Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Порядке резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

3.4. Ответственные за реагирование сотрудники ознакомляют всех сотрудников предприятия, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

3.5. По окончанию ознакомления сотрудник расписывается в журнале, предоставляемом Ответственным за реагирование сотрудником. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

3.6. Должно быть проведено обучение должностных лиц Оператора, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;

- пожаротушение;

- эвакуация людей;

- защита материальных и информационных ресурсов;

- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

- выключение оборудования, электричества, водоснабжения, газоснабжения.

3.7. Администраторы ИСПДн и Администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

3.8. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

3.9. Ответственность за организацию обучения должностных лиц несет руководитель отдела. Сроки и порядок их обучения согласуется с Администратором безопасности.