УТВЕРЖДАЮ
Главный врач
ГБУЗ «Ленинская ЦРБ»
_____Е.А.Крайнов
15.11.2013

Приложение №8
к Приказу от
15.11.2013 №515-О

Шаблоны дополнений в должностные инструкции лиц, ответственных за защиту ПДн в ГБУЗ «Ленинская ЦРБ»

Шаблоны дополнений, представленные в данном документе, должны быть добавлены в соответствующие инструкции.

1. Шаблон дополнений в инструкцию Администратора ИСПДн

Администратор Информационных систем обработки персональных данных (далее по тексту «ИСПДн») обязан:

1.1. Знать и выполнять требования действующего законодательства Российской Федерации и локальных нормативных актов Учреждения, регламентирующих вопросы защиты информации Учреждения, порядок действий по защите информации Учреждения, и т.д.

1.2. 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.

1.3. Обеспечивать работоспособность элементов ИСПДн и локальных вычислительных сетей.

1.4. Осуществлять контроль над порядком учета, создания, хранения и использования резервных и архивных копий массивов данных.

1.5. Совместно с Администратором безопасности обеспечивать функционирование и поддерживать работоспособность средств защиты информации в ИСПДн.

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

1.7. Совместно с Администратором безопасности проводить периодический контроль принятых мер защиты. Периодически осуществлять тестирование всех функций системы защиты с помощью тест-программ, имитирующих попытки НСД, при изменении программной среды и персонала ИСПДн.

1.8. Совместно с Администратором безопасности проводить периодический контроль ЛВС на предмет несанкционированных подключений (визуально, с помощью специального программного обеспечения и т. п.).

1.9. Осуществлять контроль над правильностью использования персонального пароля Пользователем ИСПДн.

1.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн, а также о других нарушениях, связанных с нарушением безопасности информации.

1.11. В случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты, информировать ответственного за обеспечение защиты персональных данных.

1.12. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации, если на них существует защищаемая информация.

1.13. Присутствовать при выполнении третьими лицами технического обслуживания элементов ИСПДн.

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

1.15. Участвовать в проведении работ по восстановлению работоспособности средств и систем защиты информации.
1.16. Осуществлять учет всех съемных электронных носителей информации с помощью их любой маркировки и с занесением учетных данных в специальный журнал. Учтенные носители информации выдавать Пользователям под роспись.
1.17. Проводить инструктаж Работников/Пользователей автоматизированных рабочих станций правилам работы с СВТ и средствами защиты информации с отметкой в карточке инструктажа.
1.18. Участвовать в разработке нормативных и методических материалов, связанных с функционированием СВТ и применением средств защиты информации, выполнением мероприятий по обеспечению защиты информации.
1.19. Планировать дальнейшее развитие структуры и функциональности ИСПДн, а также вносить предложения по совершенствованию работы и повышению эффективности функционирования средств вычислительной техники ИСПДн и системы защиты информации.
1.20. Администратор ИСПДн имеет право:
– Отключать под контролем Администратора безопасности любые элементы СЗИ ИСПДн при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей.
– При необходимости под контролем Администратора безопасности изменять конфигурацию элементов ИСПДн и СЗИ.
– Требовать от Работников Учреждения соблюдения правил работы в ИСПДн.
– Требовать от Работников Учреждения безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения требований локальных нормативных актов Учреждения, регламентирующих вопросы обеспечения безопасности и защиты информации.
– Вносить свои предложения по совершенствованию функционирования ИСПДн.

2. Шаблон дополнений в инструкцию Работника, ответственного за организацию обработки и обеспечение безопасности персональных данных (далее «ПДн»)

Работник обязан:
2.1. Знать и выполнять требования действующего законодательства Российской Федерации и локальных нормативных актов Учреждения, регламентирующих порядок использования, обработки и т.д. ПДн, защиту информации и порядок действий по защите информации, и т.д.
2.2. Контролировать установку, настройку и сопровождение технических средств защиты.
2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.
2.4. Участвовать в приемке новых программных средств.
2.5. Контролировать доступ к защищаемой информации Пользователей Информационных систем обработки персональных данных (далее по тексту «ИСПДн») согласно их правам доступа при получении оформленного соответствующим образом разрешения.
2.6. Уточнять в установленном Учреждением порядке обязанности Пользователей ИСПДн по обработке объектов защиты, а также проверять знания Пользователей в области информационной безопасности в пределах их компетенции.
2.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.
2.8. Осуществлять контроль над выполнением планов мероприятий Учреждения по защите ПДн.
2.9. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.
2.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.
2.11. Контролировать физическую сохранность средств защиты и оборудования ИСПДн с помощью программных средств и организационных мер.

2.12. Контролировать исполнение Пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты.
2.13. Контролировать исполнение Пользователями парольной политики.
2.14. Контролировать работу Пользователей в сетях общего пользования и (или) международного обмена.
2.15. Своевременно проверять журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.
2.16. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.
2.17. Контролировать допуск к работе на элементах ИСПДн посторонних лиц при проведении технического обслуживания.
2.18. Осуществлять периодические контрольные проверки автоматизированных рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.
2.19. Оказывать помощь Пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.
2.20. Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных Пользователями нарушениях установленных требований по защите информации.
2.21. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
2.22. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.
2.23. Контролировать правильность ведения журналов Учреждения:
– журнал учета обращений субъектов ПДн по выполнению их законных прав;
– журнал учета съемных носителей информации Учреждения;
– журнал учета применяемых средств защиты информации, эксплуатационной и технической документации к ним;
– журнал поэкземплярного учета применяемых средств криптографической защиты информации (далее по тексту «СКЗИ»), эксплуатационной и технической документации к ним;
– журнал учета мероприятий по контролю состояния системы защиты ПДн;
– журнал приема (сдачи) кабинетов под охрану и ключей от них;
– журнал учета мобильных технических средств;
– журнал учета сейфов и металлизированных хранилищ;
– журнал учета ключей и атрибутов доступа.
2.24. Докладывать генеральному директору Учреждения обо всех нарушениях Администраторов ИСПДн и Пользователей, связанных с защитой ПДн, а также примененные действия по устранению нарушений.
2.25. Проводить расследование при зафиксированных утечках информации.
2.26. Осуществлять взаимодействие со структурами, осуществляющими проверку состояния защищенности ПДн, в части ответов на запросы, участия в проверках, организации выполнения предписаний.
2.27. Участвовать в процессе выдачи/получения съемных носителей.

3. Шаблон дополнений в инструкцию Пользователей/Работников

Пользователь обязан:
3.1. Знать и выполнять требования действующего законодательства Российской Федерации и локальных нормативных актов Учреждения, регламентирующих вопросы защиты информации Учреждения, порядок действий по защите информации Учреждения, требования по режиму обработки персональных данных (далее по тексту «ПДн»), учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн и т.д.

3.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в правах доступа к обрабатываемым ПДн.
3.3. Соблюдать требования парольной политики Учреждения и антивирусной защиты.
3.4. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.
3.5. Использовать имеющиеся возможности, если таковые будут обеспеченны Учреждением, для размещения экрана автоматизированной рабочей станции или иного электронного носителя с ПДн на своем рабочем месте или ином месте во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией третьими лицами, закрывать шторы, жалюзи или иные закрывающие средства на оконных проемах так, чтобы исключалась возможность несанкционированного ознакомления с информацией, отображаемой на экране монитора автоматизированной рабочей станции или иного электронного носителя, третьими лицами.
3.6. Контролировать пребывание посторонних лиц (посетителей, обслуживающего персонала) в рабочем помещении для предотвращения несанкционированного доступа к информации.
3.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к Администратору безопасности любым доступным средством связи.
3.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн любым доступным средством связи.
3.9. Пользователям запрещается:
– разглашать защищаемую информацию третьим лицам;
– оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа к информационным системам Учреждения, в т.ч. ИСПДн и т.д.;
– оставлять без личного присмотра в легкодоступном месте на рабочем месте или где бы то ни было свои учтенные машинные носители и распечатки, содержащие конфиденциальную информацию (сведения ограниченного распространения), в т.ч. ПДн;
– копировать защищаемую информацию на внешние носители без разрешения своего непосредственного 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 автоматизированной рабочей станции;
– запрещено подключать к автоматизированной рабочей станции и корпоративной информационной сети личные внешние электронные 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 и должностными инструкциями;
– сообщать (или передавать) посторонним лицам личные ключи (пароли и т.д.) и атрибуты доступа к ресурсам ИСПДн;
– запрещается озвучивать защищаемую информацию (ПДн), в том числе в рабочем помещении, а также по телефонной связи;
– привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты ПДн.
3.10. При отсутствии визуального контроля над автоматизированной рабочей станцией: доступ к автоматизированной рабочей станции должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

3.11. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него должностных функций.
3.12. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться исключительно при служебной необходимости.
3.13. При работе в Сети запрещается:
– осуществлять работу при отключенных средствах защиты (антивирус и других);
– передавать по Сети защищаемую информацию – ПДн, без использования средств шифрования;
– запрещается скачивать из Сети программное обеспечение и другие файлы;
– запрещается посещение сайтов сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение и другие);
– запрещается нецелевое использование подключения к Сети.

4. Шаблон общих дополнений во все должностные инструкции Работников

4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных инструкцией, другими локальными нормативными актами Учреждения, действующего законодательства Российской Федерации, за полноту и качество проводимых им работ по обеспечению защиты информации, а также неисполнение таких обязанностей Работник Учреждения несет ответственность, предусмотренную действующим законодательством Российской Федерации.