Росгидромет
Федеральное государственное бюджетное учреждение
«ЗАПАДНО-СИБИРСКОЕ УПРАВЛЕНИЕ ПО ГИДРОМЕТЕОРОЛОГИИ И МОНИТОРИНГУ ОКРУЖАЮЩЕЙ СРЕДЫ»
(ФГБУ «Западно-Сибирское УГМС»)
10.11.2022 № 22-93

УТВЕРЖДАЮ
Начальник
_____ А.О. Люцигер
«10» 11 2022 г.
М.П.

ИНСТРУКЦИЯ
по проведению антивирусного контроля на объекте информационных систем персональных данных

1. Общие положения

1.1. Настоящая Инструкция по организации антивирусной защиты (далее - «Инструкция») разработана в соответствии со ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и определяет порядок реализации антивирусного контроля в информационных системах персональных данных ФБГУ «Западно-Сибирское УГМС» (далее – Учреждение).

1.2. Действие настоящего документа распространяется на всех работников Учреждения, выполняющих обработку персональных данных (далее - «ПДн») в ИСПДн, и на администратора информационной безопасности (далее – ИБ).

1.3. Непосредственное руководство проведением работ по антивирусной защите осуществляет назначенный администратором ИБ работник ЗС РВЦ.

1.4. Ответственность за проведение мероприятий антивирусного контроля в Учреждении, выполнение мероприятий по антивирусной защите ПДн на эксплуатируемых средствах вычислительной техники возлагается на администратора ИБ.

1.5. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты ПДн и требований настоящей Инструкции несут работники, за которыми закреплены соответствующие рабочие станции.

1.6. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в три года.

2. Правила проведения антивирусного контроля

2.1. ИСПДн запрещается установка программного обеспечения, не связанного выполнением функций, предусмотренных технологическим процессом обработки информации на рабочих станциях.

2.2. В случае если пользователю ИСПДн разрешено применение съемных машинных носителей информации, он обязан перед началом работы осуществить проверку их на предмет отсутствия компьютерных вирусов.

2.3. Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы.

2.4. При обнаружении компьютерного вируса пользователи обязаны немедленно поставить в известность администратора ИСПДн или администратора безопасности и прекратить какие-либо действия с информационными ресурсами ИСПДн.

2.5. Администратор ИБ проводит расследование факта заражения ИСПДн компьютерным вирусом. Лечение зараженных файлов осуществляется путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводится антивирусный контроль.

2.6. Обо всех фактах заражения администратор ИБ обязан ставить в известность ответственного за обеспечение безопасности ПДн.

2.7. Установка и настройка параметров средств антивирусного контроля на средствах вычислительной техники ИСПДн осуществляется в соответствии с программной и эксплуатационной документацией, поставляемой вместе с ними.

2.8. Обязательному входному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, входящие в состав ИСПДн, программные средства общего и специального назначения, любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по каналам передачи данных, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM, Flash-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед ее отправкой (записью на съемный носитель).

2.9. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.10. Периодическая проверка жестких магнитных дисков на отсутствие программных вирусов должна проводиться не реже одного раза в неделю. Обязательная проверка используемых в работе гибких магнитных дисков должна осуществляться перед началом работы с ними.

2.11. При повреждении программных средств и информационных массивов программными вирусами должны выполняться мероприятия по восстановлению их работоспособности.

3. Правила обновления баз данных вирусных описаний

3.1. Обновление баз данных вирусных описаний средств антивирусной защиты, используемых для защиты серверов, рабочих станций, а также периметральных средств защиты информации (средств межсетевого экранирования, прокси-серверов, почтовых шлюзов и других средств защиты информации при наличии технической возможности установки антивирусной программы на данные средства) должно осуществляться централизовано администратором ИБ без участия пользователей посредством механизма централизованного управления и обновления баз данных вирусных описаний.

3.2. Для осуществления процедуры копирования антивирусных обновлений с серверов обновлений, находящихся в сети Интернет, необходимо использовать отдельное выделенное рабочее место. После этого новые антивирусные базы могут быть скопированы в общедоступную папку.

3.3. Процедура обновления антивирусных баз должна проводиться не реже одного раза в неделю.

3.4. Для рабочих станций, являющихся автономными с точки зрения централизованного управления, обновление баз данных вирусных описаний должно осуществляться непосредственно самими работниками структурных подразделений, за которыми закреплен данный компьютер. В качестве источника обновлений может выступать общая папка, содержащая необходимые файлы, на одном из компьютеров ИСПДн.

4. Правила проведения антивирусной проверки

4.1. Установка (изменение) системного и прикладного программного обеспечения должна осуществляться в соответствии с программной и эксплуатационной документацией, поставляемой вместе с ним. Устанавливаемое (изменяемое) программное обеспечение

должно быть предварительно проверено администратором ИСПДн или администратором безопасности. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена полная антивирусная проверка компьютера администратором ИБ.

4.2. Сканирование рабочих станций пользователей средствами антивирусной защиты производится централизовано, не реже одного раза в неделю.

4.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно или совместно с администратором ИБ должен провести внеочередной антивирусный контроль своего персонального компьютера.

4.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- принять меры по локализации программного вируса (отключить персональный компьютер от локальной вычислительной сети);
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора ИБ, руководителя подразделения, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с администратором ИБ и владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- по возможности провести лечение зараженного файла. В случае невозможности вылечить зараженный файл, необходимо поместить его в карантин, и выполнить процедуру по восстановлению незараженной копии исходного файла из имеющегося архива.

4.5. В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, администратор ИБ должен:

- заархивировать зараженные файлы с внедренными программными вирусами и направить данный архив в организацию, с которой заключен договор технической поддержки эксплуатации средств антивирусной защиты (при необходимости, для выполнения требований данного пункта привлечь специалиста по защите информации);

4.6. По факту обнаружения зараженных вирусом файлов администратор ИБ должен составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.