УТВЕРЖДЕНА

приказом директора
ОГБУ «КЦСО ЕАО»
от «02» 07 2024 г. № 184

ИНСТРУКЦИЯ
по организации антивирусной защиты в ИСПДн областного государственного бюджетного учреждения «Комплексный центр социального обслуживания Еврейской автономной области»

1. Общие положения

1.1. Настоящая Инструкция по антивирусной защите (далее – Инструкция) в информационной системе персональных данных (далее – ИСПДн) областного государственного бюджетного учреждения «Комплексный центр социального обслуживания Еврейской автономной области» (далее – ОГБУ «КЦСО ЕАО», Учреждение) регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля. Инструкция устанавливает требования и ответственность при организации защиты информации от разрушающего воздействия вредоносных программ – компьютерных вирусов.

1.2. Инструкция предназначена для администратора информационной безопасности, специалиста по технической поддержке и пользователей, обрабатывающих персональные данные на автоматизированных рабочих местах (далее АРМ) в ОГБУ «КЦСО ЕАО».

1.3. Инструкция распространяется на все АРМ сотрудников Учреждения и обязательна к использованию во всех структурных подразделениях.

1.4. Указанные в настоящей Инструкции правила и требования должны применять все сотрудники ОГБУ «КЦСО ЕАО», использующие в своей работе автоматизированные рабочие места в соответствии и в рамках своих должностных обязанностей.

2. Нормативные ссылки

Настоящая инструкция составлена на основе следующих нормативных документов:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Требования к антивирусным средствам

3.1 К применению на АРМ допускаются только лицензионные антивирусные программные и (или) программно-аппаратные средства (антивирусные средства).

3.2 Антивирусные средства должны функционировать в течение всего времени работы средств вычислительной техники (от момента загрузки операционной системы до момента её выгрузки).

3.3 Антивирусное средство не должно существенно затруднять работоспособность средств вычислительной техники ИСПДн.

3.4. Периодичность обновления антивирусных баз:

- обновление антивирусных баз для всех ИСПДн, имеющих подключение к сетям общего пользования и сетям международного информационного обмена, должно быть ежедневным. Источник обновления – сервер разработчика антивирусного средства, либо собственный централизованный сетевой источник обновлений, получающий обновления с сервера разработчика антивирусного средства.

- обновление антивирусных баз для ИСПДн, не имеющих подключение к сетям общего пользования и сетям международного информационного обмена, обновление должно быть не менее 1 раза в неделю. Источником обновления в данном случае являются антивирусные базы, записанные на предварительно учтённый в установленном порядке съёмный машинный носитель информации. Ответственный один раз в неделю осуществляет установку пакетов обновлений антивирусных баз, осуществляет контроль их подключения к антивирусному программному обеспечению и проверку жёсткого диска и съемных носителей на наличие вирусов.

4. Права и обязанности

4.1. Антивирусной защите подлежит вся, обрабатываемая в Учреждении при помощи средств вычислительной техники информация, независимо от ограничений доступа к ней.

4.2. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

4.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

4.4. На АРМ запрещается установка программного обеспечения, не связанного с выполнением функций Учреждения.

4.5. Ответственность за организацию антивирусной защиты в ИСПДн и за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля (регулярное обновление, выявление фактов заражения, «лечение» зараженных файлов) возлагаются на администратора информационной безопасности, специалиста по технической поддержке.

4.6. Основные задачи по обеспечению антивирусной защиты в ИСПДн:

- организация процесса установки антивирусных средств в ИСПДн;

- сопровождение антивирусных средств (обновление, антивирусный контроль, сопровождение действий пользователей в случаях обнаружения вирусов, обеспечение работоспособности антивирусных средств);

- контроль состояния системы антивирусной защиты информации в Учреждении.

4.7. Ответственный за обеспечение антивирусной защиты в ИСПДн и проведение антивирусного контроля несёт ответственность:

- за своевременную установку антивирусных средств;

- за эксплуатацию (антивирусный контроль, работоспособность антивирусных средств, сопровождение действий пользователей в случаях обнаружения вирусов) системы антивирусной защиты информации;

- за своевременное обновление лицензий на антивирусные средства;

- за своевременное обновление антивирусных баз.

4.8. Ответственный за обеспечение антивирусной защиты в ИСПДн и проведение антивирусного контроля имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации;

- принимать участие в планировании мероприятий по антивирусной защите информации и планировании оснащения антивирусными средствами;

- осуществлять контроль состояния средств антивирусной защиты информации в Учреждении;

- инициировать служебные проверки и участвовать в проведении расследований по фактам заражения вирусами ИСПДн и средств вычислительной техники;

- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты.

4.9. Пользователь антивирусного средства – специалист, на рабочем месте которого применяется антивирусное средство.

4.10. Пользователям антивирусных средств запрещается:

- менять настройки или отключать средства антивирусной защиты во время работы;

- использовать средства антивирусной защиты, отличные от установленных средств;

- без разрешения администратора информационной безопасности копировать любые файлы на съёмные носители информации, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

5. Порядок действий при обнаружении вирусов

5.1. Основными путями проникновения вирусов в ИСПДн являются: любые съёмные машинные носители информации, электронные почтовые сообщения, трафик, получаемый из сетей общего пользования и сетей международного информационного обмена, ранее зараженные рабочие станции и сервера.

5.2. Пользователи АРМ при работе с носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

5.3. В случае обнаружения вирусов при входном контроле съёмных машинных носителей информации, файлов или электронных почтовых сообщений, пользователь должен:

- немедленно приостановить все работы на своём АРМ;

- сообщить ответственному за обеспечение антивирусной защиты в ИСПДн о факте обнаружения вируса;

- принять согласованные с ответственным за обеспечение антивирусной защиты в ИСПДн меры по локализации и удалению вируса с использованием антивирусных средств.

5.4. Ответственный проводит расследование факта заражения АРМ компьютерным вирусом. «Лечение» зараженных файлов осуществляется путём выбора соответствующего пункта меню антивирусной программы и после этого вновь проводится антивирусный контроль.

5.5. В случае обнаружения вируса, не поддающегося лечению, ответственный обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность АРМ. В случае отказа АРМ – произвести восстановление соответствующего программного обеспечения.

5.6. Обо всех фактах заражения АРМ, ответственный обязан ставить в известность ответственного за организацию обработки персональных данных

и своего непосредственного руководителя.

5.7. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на АРМ данного пользователя незамедлительно блокируется по решению ответственного за обеспечение безопасности ПДн в ИСПДн.

5.8. Факты модификации и разрушения данных на АРМ, заражение их вирусами, а также обнаружение других вредоносных программ – все это относится к значимым нарушениям безопасности информации и должны быть проанализированы посредством проведения служебного расследования.

5.9. Служебное расследование проводится комиссией, назначаемой приказом директора Учреждения. В состав комиссии в обязательном порядке включается ответственный за организацию обработки ПДн, администратор информационной безопасности, непосредственный руководитель работника, допустившего факт компрометации. При необходимости в состав комиссии могут включаться другие работники.

5.10. Результаты работы комиссии оформляются актом.

6.Заключительные положения

2.1. Настоящая Инструкция вступает в силу в силу с момента утверждения приказа руководителем Учреждения.

2.2. Срок действия настоящей Инструкции не ограничен.

2.3. По мере необходимости в настоящую Инструкцию могут быть внесены дополнения и изменения в соответствии с законодательством РФ.