Приложение 5
к приказу ГБОУ ОЦДиК
от 29.12.2017 г.№ 245

Инструкция
по организации антивирусной защиты

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с нормативными документами по безопасности информации и определяет требования к организации защиты информационной системы персональных данных (далее – ИСПДн) ГБОУ «Областной центр диагностики и консультирования» (далее – Учреждение) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность администратора безопасности (далее – АБ) за выполнение указанных требований.

1.2. К использованию в Учреждении допускаются только лицензионные средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

1.3. Установка средств антивирусного контроля на компьютеры и серверы ИСПДн Учреждения осуществляется АБ или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Антивирусная защита – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.

2.2. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.3. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.4. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

3. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

3.1. Антивирусный контроль должен осуществляться в режиме постоянной антивирусной защиты. Ежедневно в начале работы при загрузке компьютера (для серверов – при перезапуске) в автоматическом режиме должна проводиться проверка загружаемых модулей операционной системы.

3.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после ее приема.

3.3. Процедура обновления баз данных средства антивирусной защиты должна проводиться не реже одного раза в день на всех АРМ ИСПДн, работающих в сети, не реже одного раза в неделю для всех АРМ ИСПДн, работающих автономно.

3.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено АБ на предмет отсутствия вредоносного программного обеспечения. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка на всех защищаемых серверах и АРМ ИСПДн.

3.5. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) пользователь обязан самостоятельно или вместе с АБ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля – уведомить о результатах АБ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственность за проведение мероприятий антивирусного контроля и настройку средств антивирусного контроля в ИСПДн Учреждения в соответствии с требованиями настоящей Инструкции возлагается на АБ.

4.2. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИСПДн Учреждения, осуществляется АБ.