Приложение № 1

Утверждено

приказом государственной

инспекции по охране объектов

культурного наследия

Новосибирской области

от \_\_\_\_\_\_ 2023 г. № \_\_\_\_\_

Инструкция

по организации антивирусной защиты в информационных системах персональных данных

1. Общие требования

1.1. Настоящая Инструкция по организации антивирусной защиты в информационных системах персональных данных (далее – Инструкция) определяет требования к организации защиты информационных систем персональных данных (далее – ИСПДн) государственной инспекции по охране объектов культурного наследия Новосибирской области) (далее – ГИО ОКН НСО) от разрушающего воздействия вредоносных компьютерных программ (компьютерных вирусов) и устанавливает ответственность сотрудников ГИО ОКН НСО, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. К использованию в ИСПДн допускаются только средства антивирусной защиты прошедшие в установленном порядке процедуру оценки соответствия.

1.3. Установка и настройка средств антивирусной защиты осуществляется специально назначенным лицом (администратором безопасности информации), в соответствии с руководствами по применению конкретных средств антивирусной защиты.

2. Применение средств антивирусной защиты

2.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных машинных носителях (USB «флэш»-накопителях, накопителях на гибких магнитных дисках, оптических компакт-дисках и прочие) перед копированием в ИСПДн.

2.2. Накопители на жестких дисках, и оперативная память АРМ должны находятся под постоянным контролем средства антивирусной защиты.

2.3. Полная проверка всех файлов ИСПДн должна выполняться по расписанию не реже одного раза в неделю, а также по запросу пользователя ИСПДн.

2.4. Быстрая проверка файлов ИСПДн должна выполняться автоматически после запуска средства антивирусной защиты.

2.5. Должна проводиться автоматическая проверка подключаемых съемных машинных носителей.

2.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения автоматизированного рабочего места (далее - АРМ), администратором безопасности информации должна быть выполнена антивирусная проверка соответствующего АРМ.

2.7. 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 ИСПДн самостоятельно или вместе с администратором безопасности информации должен провести внеочередную антивирусную проверку своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИСПДн обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности информации;

провести анализ необходимости дальнейшего использования зараженных файлов;

провести лечение или уничтожение зараженных файлов.

2.8. Обновление базы данных признаков вредоносных компьютерных программ средства антивирусной защиты должно осуществляться не реже чем один раз в два часа в автоматическом режиме со специального сервера обновлений средства антивирусной защиты.

3. Ответственность

3.1. Ответственность за организацию и проведение мероприятий по антивирусной защите в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности информации.

3.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников ГИО ОКН НСО, являющихся пользователями ИСПДн.

3.3. Периодический контроль за состоянием антивирусной защиты в ИС АП ЕГИСМ, а также за соблюдением установленного порядка антивирусной защиты и выполнением требований настоящей Инструкции осуществляется администратором безопасности информации.