Приложение №14

УТВЕРЖДЕНА
распоряжением
администрации
от 23.04.2024 № 82

ИНСТРУКЦИЯ

по организации антивирусной защиты в информационных системах персональных данных администрации муниципального образования «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области

1. Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты в информационных системах персональных данных (далее –ИСПДн) и устанавливает ответственность за их выполнение.

2. Основные определения

Вредоносное программное обеспечение (далее ПО) - специально разработанное программное обеспечение, программный модуль, блок, группа команд, имеющая способность к самораспространению, которая может попадать в общее и специальное программное обеспечение ИСПДн и приводить к:

- дезорганизации вычислительного процесса (нарушению или существенному замедлению обработки информации);
- модификации или уничтожению программ, или данных;
- приведению в негодность носителей информации и других технических средств;
- нарушению функционирования средств защиты информации.

3. Инструкция по применению средств антивирусной защиты

Защита ПО ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

1.1. К использованию допускаются только лицензионные антивирусные средства, обладающие необходимой сертификацией в регулирующих органах РФ.

1.2. Решение задач по установке и сопровождению средств антивирусной защиты возлагается на администратора безопасности ИСПДн.

1.3. Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.

1.4. Всё впервые вводимое в эксплуатацию ПО должно проходить обязательный антивирусный контроль.

1.5. Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места администратора безопасности ИСПДн.

1.6. Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ИСПДн.

1.7. Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов ИСПДн.

1.8. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.

1.9. Контроль входящей информации необходимо проводить непосредственно после ее приема.

1.10. Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

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

1.12. 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, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться к администратору безопасности ИСПДн.

1.13. При получении информации о возникновении вирусной эпидемии вне ИС должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.

1.14. В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса администратора безопасности ИСПДн;
- провести лечение зараженных файлов;
- в случае невозможности лечения обратиться к администратору безопасности ИСПДн.

1.15. По факту обнаружения зараженных вирусом файлов администратор безопасности ИСПДн 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.

1.16. Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.

1.17. Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

1.18. Администратор безопасности ИСПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.

1.19. С данной инструкцией Пользователи должны быть ознакомлены под роспись в листе ознакомления с данной инструкцией.

1.20. Проводить периодическое тестирование функций средств антивирусной защиты.

1.21. Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).