УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ КРАСНЫЙ ЯР МУНИЦИПАЛЬНОГО РАЙОНА КРАСНОЯРСКИЙ САМАРСКОЙ 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.

- К использованию допускаются только лицензионные антивирусные средства, обладающие необходимой сертификацией в регулирующих органах РФ.
- Решение задач по установке и сопровождению средств антивирусной защиты возлагается на системного администратора Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .
- Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.
- Всё впервые вводимое в эксплуатацию ПО должно проходить обязательный антивирусный контроль.
- Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места системного администратора Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области .
- Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ИСПДн.
- Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов ИСПДн.
- 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.
- Контроль входящей информации необходимо проводить непосредственно после ее приема.
- Контроль исходящей информации необходимо проводить непосредственно перед отправкой.
- Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

- 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 системному администратору Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области.
- При получении информации о возникновении вирусной эпидемии вне ИС должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.
- В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса системного администратора Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области;
- провести лечение зараженных файлов;
- в случае невозможности лечения обратиться к администратору безопасности ИСПДн.

- По факту обнаружения зараженных вирусом файлов системный администратор Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области 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.
- Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.
- Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
- Ответственный за организацию обработки ПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.
- С данной инструкцией Пользователи должны быть ознакомлены под подпись в листе ознакомления с данной инструкцией.
- Проводить периодическое тестирование функций средств антивирусной защиты.
- Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).