ПРИЛОЖЕНИЕ № 13
К ПРИЗАЗУ МАОУ «СОШ № 2»
«ОБ УТВЕРЖДЕНИИ ПОЛИТИКИ
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ»
ОТ 03.10.2023 № 390

ИНСТРУКЦИЯ ПО АНТИВИРУСНОЙ ЗАЩИТЕ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения.

Инструкция по проведению антивирусного контроля МАОУ «Средняя о4бщеобразовательная школа № 2» (далее – Организация) устанавливает порядок организации защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (ПО) и устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих ИСПДн.

Требования настоящего документа распространяются на всех сотрудников Организации, использующих в работе ИСПДн. В целях закрепления знаний по вопросам практического исполнения требований данного порядка ответственным за информационную безопасность проводятся периодические инструктажи.

2. Применение средств антивирусной защиты.

На всех АРМ и серверах ИСПДн должны использоваться только лицензионные и сертифицированные ФСТЭК России средства антивирусной защиты (Dr. Web или Kaspersky Antivirus). Установка средств антивирусной защиты должна осуществляться только с сертифицированных ФСТЭК России дистрибутивов, не допускается установка антивирусных средств с дистрибутивов, полученных из сети Интернет (либо иным способом).

Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой. Обновление антивирусных баз должно быть настроено на автоматическое обновление. Обновление баз антивирусных средств должно проводиться регулярно в автоматическом режиме, для чего администратором безопасности должен быть настроен доступ к серверам обновлений разработчика антивирусного средства. В случае невозможности настроить доступ к серверам обновлений разработчика антивирусного средства, администратор безопасности должен один раз в неделю осуществлять установку пакетов обновлений вирусных баз, контроль их подключения к антивирусному пакету и проверку АРМ и серверов ИСПДн на наличие вирусов.

3. Функции администратора безопасности по обеспечению антивирусной безопасности.

Администратор информационной безопасности обязан:

– проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты;

– устанавливать и настраивать параметры средств антивирусной защиты в соответствии с эксплуатационной документацией;

– предварительно проверять устанавливаемое (обновляемое) ПО на отсутствие вирусов;

– обеспечивать бесперебойное функционирование системы антивирусной защиты;

– разрабатывать дополнительные инструкции по работе пользователей с программными средствами антивирусной защиты;
– проводить работы по обнаружению и обезвреживанию вирусов;
– участвовать в работе комиссии по расследованию причин заражения АРМ и серверов;
– хранить эталонные копии антивирусных программных средств;
– осуществлять периодический (не реже 1 раза в 3 месяца) контроль за соблюдением пользователями АРМ требований настоящего порядка;
– заполнять журнал учета нештатных ситуаций;
– проводить восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами;
– принимать участие в служебных расследованиях по фактам заражения вредоносными программами информационных ресурсов ИСПДн;
– проводить периодический (не реже 1 раза в 3 месяца) контроль работы программных средств системы антивирусной защиты информации на АРМ.

4. Функции пользователей ИСПДн.

Пользователи ИСПДн:
– не должны принудительно отключать средства антивирусной защиты на АРМ;
– не должны изменять настройки и конфигурацию средств антивирусной защиты;
– не должны удалять или добавлять в систему какие-либо другие средства антивирусной защиты;
– не должны использовать на АРМ съемные носители информации без предварительной проверки установленными средствами антивирусной защиты;
– не должны запускать неизвестные приложения, пришедшие по электронной почте;
– 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.) сотрудник самостоятельно или вместе с администратором безопасности должен провести внеочередную антивирусную проверку АРМ. При необходимости Пользователь ИСПДн должен привлечь администратора безопасности для определения факта наличия или отсутствия компьютерного вируса;
– в случае обнаружения зараженных компьютерными вирусами файлов при проведении повторной антивирусной проверки сотрудники
обязаны:
• приостановить работу;
• немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, владельца зараженных файлов;
• совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
• провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора безопасности);
• по факту обнаружения зараженных вирусом файлов составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.
– в случае, когда антивирусному средству удалось полностью вылечить/удалить зараженный объект, пользователь перезагружает свой ПК и запускает полную проверку системы на наличие вредоносных программ;
– если зараженные файлы отсутствуют, пользователь может вернуться к исполнению своих служебных обязанностей.

5. Ответственные за организацию и контроль выполнения документа.

Ответственность за организацию контрольных и проверочных мероприятий по вопросам антивирусной защиты возлагается на администратора безопасности. Руководители структурных подразделений несут ответственность за выполнение мероприятий по антивирусной защите информации на АРМ, эксплуатируемых подчиненными сотрудниками в своем структурном подразделении. Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности и обработку ПДн объекта автоматизации.