Согласовано
Председатель профкома:
_____ Касаткина О.В.
Протокол № 11 от 29.08.2014г.

Утверждаю
Директор МОУ Иванковской СОШ:
_____ Г.В. Жаренова
Приказ № 175 от 01.09.2014г

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ ОБЪЕКТА АВТОМАТИЗАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Инструкция по организации антивирусной защиты в информационных системах персональных данных (ИСПДн) МОУ Иванковской СОШ (далее – Учреждение) определяет требования к организации защиты объектов автоматизации от вредоносного воздействия компьютерных вирусов и устанавливает ответственность сотрудников, допущенных в силу своих служебных (функциональных) обязанностей к автоматизированной обработке персональных данных в ИСПДн.

Инструкция распространяется на автоматизированные системы, предназначенные для обработки информации ограниченного распространения (персональных данных).

2. В ИСПДн Учреждения допускается использование только лицензионных антивирусных средств, официально приобретенных у разработчиков (поставщиков) антивирусного программного обеспечения, и прошедшие в установленном порядке процедуру оценки соответствия требованиям по безопасности.

3. Установка (изменение) и настройка системного и прикладного программного обеспечения, а также средств антивирусного контроля на автоматизированных рабочих местах (АРМ) и ИСПДн Учреждения осуществляется Администратором ИСПДн и (или) Администратором безопасности ИСПДн на основании «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы».

4. Настройка параметров средств антивирусного контроля осуществляется Администратором ИСПДн и (или) Администратором безопасности ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств.

2. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

1. Антивирусный контроль всех дисков и файлов АРМ должен проводиться ежедневно в начале работы в автоматическом режиме при загрузке компьютера, а для серверов - при перезапуске.

2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (флэш-устройствах памяти, магнитных дисках, лентах, CD - ROM и т.п.).

3. Настройка средств антивирусной защиты должна реализовывать следующие функции:

- непрерывный автоматический мониторинг информационного обмена в ИСПДн с целью выявления программно-математического воздействия (далее – ПМВ);
- автоматическая проверка на наличие вредоносных программ или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа;
- реализация механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;

− автоматическая проверка критических областей автоматизированных рабочих мест и серверов, таких как системная память, загрузочные секторы дисков, объекты автозапуска, каталоги операционной системы «system» и «system32» при каждом запуске операционной системы;

− полная автоматическая проверка носителей информации всех АРМ и серверов не реже одного раза в неделю;

− регулярное обновление антивирусных баз и программных модулей средств антивирусной защиты;

− автоматическое документирование состояния системы антивирусной защиты ИСПДн.

3. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

5. Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы.

6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения на АРМ должна быть выполнена антивирусная проверка электронных средств обработки.

3. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ВИРУСОВ

1. 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 АРМ самостоятельно или вместе с Администратором ИСПДн и (или) Администратором безопасности ИСПДн должен провести внеочередной антивирусный контроль своей рабочей станции.

2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь АРМ обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора ИСПДн и (или) Администратора безопасности ИСПДн и непосредственного руководителя;
- по согласованию с Администратором ИСПДн и (или) Администратором безопасности ИСПДн провести анализ необходимости дальнейшего использования зараженных вирусом файлов;
- провести лечение или уничтожение зараженных файлов.

4. ОТВЕТСТВЕННОСТЬ

1. Ответственность за организацию антивирусного контроля в Учреждении возлагается на Администратора безопасности ИСПДн и Администратора ИСПДн.

2. Ответственность за соблюдение требований настоящей Инструкции возлагается на руководителей подразделений и всех пользователей ИСПДн.

3. Периодический контроль состояния антивирусной защиты, а также соблюдения установленного порядка антивирусного контроля и выполнения требований настоящей Инструкции пользователями ИСПДн осуществляется Администратором ИСПДн, Администратором безопасности ИСПДн и комиссией, назначенной с целью, проверки соответствия требований законодательства Российской Федерации в области персональных данных.

Принято на заседании общего собрания
работников МОУ Иванковской СОШ
Протокол № 1 от 27.08. 2014г