Администрация городского округа Клин
Муниципальное бюджетное образовательное учреждение дополнительного образования «ВЫСОКОВСКАЯ ДЕТСКАЯ ШКОЛА ИСКУССТВ» (МБОУ ДО ВДШИ)

141650, МО, Клинский район, г. Высоковск, ул. Ленина, д. 9Д
E-mail: VDSHI_KLIN@mail.ru
www.vysdshi.ru
тел./факс (49624) 6-23-44

Приказ № 75 ОД

«Об утверждении Политики антивирусной защиты информационных систем в МБОУ ДО ВДШИ» **от 28.11.2018 г.**

В соответствии с Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации» и в целях совершенствования системы защиты информации в муниципальном бюджетном образовательном учреждении дополнительного образования «Высоковская детская школа искусств»:

1. Утвердить прилагаемую Политику антивирусной защиты информационных систем в МБОУ ДО ВДШИ (приложение №1);
2. Комлевой Е.В., заместителю директора по КВР, опубликовать информацию на официальном сайте МБОУ ДО ВДШИ.

Директор МБОУ ДО ВДШИ Е.М.Сорокина

Приложение № 1

ПОЛИТИКА
антивирусной защиты информационных систем
в МБОУ ДО ВДШИ

Перечень используемых сокращений

АРМ-автоматизированное рабочее место;

ИОД-информация ограниченного доступа (информация, доступ к которой должен быть ограничен в соответствии с законодательством Российской Федерации);

ИС - информационная система;

МНИ - машинный носитель информации;

ПДн - персональные данные;

ПО - программное обеспечение;

САЗ – средство антивирусной защиты;

СВТ – средство вычислительной техники;

ОМСУ – МБОУ ДО «Высоковская детская школа искусств»

I. Общие положения

1. Настоящая Политика антивирусной защиты информационных систем в МБОУ ДО ВДШИ (далее – Политика) определяет состав и порядок мероприятий по антивирусной защите ИС ОМСУ и СВТ работников ОМСУ.

2. Политикой не охватываются вопросы защиты СВТ, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну.

3.Положения Политики должны учитываться при определении правил и разработке инструкций по проведению антивирусной защиты ИС ОМСУ.

4. В Политике учтены требования следующих нормативных правовых актов и методических документов в области защиты информации:

Федеральный закон от 27.07.2006 №149-ФЗ «об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;

Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Указ Президента Российской Федерации от 17.03.2008 №351 «О мерах по обеспечению информационной безопасности Российской федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

Приказ ФСБ России и ФСТЭК России от 31.08.2010 №416/489 «Об утверждении требований к защите информации, содержащейся в информационных системах общего пользования»;

Приказ ФСТЭК России от 20.03.2012 №28 «Об утверждении требований к средствам антивирусной защиты»;

Приказ ФСТЭК России от 11.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Приказ ФСТЭК России от 18.02.2013 № «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11.02.2014;

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждён решением представителя Гостехкомиссии России от 30.03.1992;

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) утверждены приказом Гостехкомиссии России от 30.08.2002 №282.

5 Антивирусная защита достигается путём:

Эксплуатации САЗ;

Поддержания в актуальном состоянии баз вирусных сигнатур САЗ.

6. В целях исполнения Политики в каждом ОМСУ должны быть разработаны с учётом положений Политики и утверждены руководителем ОМСУ инструкции по антивирусной защите информации в ИС ОМСУ.

7. Требования к осуществлению антивирусной защиты каждой отдельной ИС ОМСУ должны определяться индивидуально с учётом положений настоящей Политики и должны учитывать особенности технологического процесса обработки

информации в этой системе, топологию ИС, а также максимальную разрешённую категорию обрабатываемой информации.

8. Антивирусная защита каждой отдельной ГИС, ИС ОМСУ, предназначенной для обработки ПДН и (или) иной ИОД либо иной защищаемой информации, обладателями которой являются ОМСУ, должна осуществляется посредством сертифицированных в установленном порядке на соответствии требованиям по безопасности информации САЗ.

9. Требования к осуществлению антивирусной защиты каждой отдельной ИС ОМСУ из указанных в п. 8 Политики должны оформляться в виде «Инструкции по обеспечению антивирусной защиты в ИС» и утверждаться в установленном порядке.

II. Выбор средств антивирусной защиты информации

10. САЗ должны использоваться во всех сегментах ИС ОМСУ и на СВТ работников ОМСУ независимо от наличия в них ИОД.

11. Допускается не применять САЗ на СВТ, не имеющих сетевых подключений, технологический процесс обработки информации

12. САЗ, применяемые в ИС, указанных в п.8 Политики, должны иметь действующие сертификаты соответствия требованиям безопасности.

13. Выбор САЗ для каждой конкретной ИС, указанной в п.8 Политики, должен производится ответственным за защиту информации в ОМСУ в зависимости от топологии ИС и категории обрабатываемой в ней информации в соответствии с требованиями нормативных правовых актов и методических документов в области защиты информации.

III. Порядок использования САЗ информации в информационных системах ОМСУ

14. Порядок использования САЗ определяется эксплуатационной документацией конкретного САЗ, инструкцией по антивирусной защите в ОМСУ, а также инструкцией по антивирусной защите ОМСУ (при её наличии).

15. Установка и сопровождение, а также периодическое обновление баз вирусных сигнатур САЗ, выполняется администратором безопасности ИС, либо (в ИС, не предназначенных для обработки ИОД) специалистом, ответственным за техническое обслуживание ИС.

16. Периодичность обновления баз вирусных сигнатур САЗ должна определяться периодичностью выхода официальных обновлений баз. В случае невозможности автоматического обновления баз вирусных сигнатур САЗ проверка наличия обновлений и обновления баз вирусных сигнатур САЗ должны осуществляется администратором безопасности ИС либо (в ИС, не предназначенных для обработки ИОД) специалистом, ответственным за техническое обслуживание ИС, не реже одного раза в неделю в ручном режиме. В случае выхода критических

обновлений баз вирусных сигнатур САЗ их установка должна производится незамедлительно.

17. Пи эксплуатации САЗ в ОМСУ должны выполняться следующие требования:

Должна обеспечивается проверка на отсутствие вредного ПО всей поступающей в ИС информации, как по каналам связи (в том числе по электронной почте), так и на съёмных МНИ;

Должна производится периодическая проверка не съёмных МНИ на отсутствие вредоносного ПО;

Антивирусный контроль в ИС должен осуществляется постоянно в автоматическом режиме.

18. В случаях:

Выявления факта заражения ресурсов ИС;

Подозрения на заражение ресурсов ИС вредоносным ПО;

Получения предупреждения о повышенной вирусной активности;

19. При возникновении подозрения на наличие вредоносного ПО пользователь самостоятельно должен провести внеочередную проверку своего СВТ на наличие вредоносного ПО.

20. При обнаружении вредоносного ПО пользователь обязан доложить о факте заражения СВТ администратору безопасности ИС или лицу, ответственному за защиту информации ОМСУ, либо специалистам, ответственным за техническое обслуживание ИС (в ИС, не предназначенных для обработки ИОД), после чего ими должны быть приняты меры по антивирусной защите, восстановлению повреждённых файлов и восстановлению работоспособности ИС. Информация об инциденте должна быть доведена до руководства ОМСУ в установленном порядке.

21. Запрещается эксплуатация сегмента ИС либо СВТ при выявлении в нем вредоносного ПО до момента локализации угрозы и восстановления работоспособности соответствующего сегмента ИС либо СВТ.

22. При обнаружении вредоносного ПО на СВТ, имеющих сетевые подключения, необходимо отключить их от локальной вычислительной сети до момента локализации угрозы и восстановления работоспособности соответствующего СВТ.

23. При обнаружении вредоносного ПО в информации, поступившей по каналам связи или со съёмных МНИ из других ОМСУ либо иных организаций, необходимо сообщить об этом факте лицу, ответственному за защиту информации вышеупомянутой организации (ведомства).

IV. Реализация Политики в ОМСУ

24. Реализация Политики в ОМСУ осуществляется за счёт согласованных действий руководителя ОМСУ, лиц, ответственных за защиту информации в ОМСУ, администраторов безопасности ИС, специалистов ОМСУ.

25. Руководитель ОМСУ:

Назначает ответственного (ответственных) за обеспечение защиты информации в ОМСУ соответствующим приказом;

Назначает администраторов безопасности ИС ОМСУ соответствующими приказами (при необходимости);

Утверждает инструкцию по обеспечению антивирусной защиты информации в ОМСУ;

Утверждает инструкции по обеспечению антивирусной защиты информации в ИС ОМСУ (при необходимости);

Осуществляет контроль за исполнением Политики в ОМСУ;

Организует расследования инцидентов, связанных с нарушениями Политик в ОМСУ;

Устанавливает ответственность работников ОМСУ за нарушение Политики;

Оповещает Мингосуправления Московской области о выявленных в ОМСУ инцидентах информационной безопасности, связанных с вредоносным ПО;

Соблюдает требования законодательства Российской Федерации и Московской области, положения Политики, инструкции по обеспечению антивирусной защиты в ОМСУ, а также инструкций по обеспечению антивирусной защиты в ИС (при их наличии);

Обеспечивает исполнение требований законодательства Российской Федерации и Московской области, положений Политики, инструкции по обеспечению антивирусной защиты в ИС (при их наличии), работниками ОМСУ.

26. Ответственный за обеспечение защиты информации в ОМСУ:

Осуществляет контроль за действиями администраторов безопасности ИС и специалистов, ответственных за техническое обслуживание ИС (в части исполнения положений Политики);

Организует проведение периодического контроля соблюдения требований информационной безопасности в ОМСУ в части антивирусной защиты информации;

Проводит сбор и анализ информации об инцидентах информационной безопасности, связанных с нарушениями Политики в ОМСУ;

Проводит расследование инцидентов, связанных с нарушениями Политики в ОМСУ;

Соблюдает требования законодательства Российской федерации и Московской области, положения Политики, инструкции по обеспечению антивирусной защиты в ОМСУ, а также инструкций по обеспечению антивирусной защиты в ИС (при их наличии);

Осуществляет контроль исполнения требований законодательства Российской Федерации и Московской области, положений Политики, инструкции по обеспечению антивирусной защиты в ОМСУ, а также инструкций по обеспечению антивирусной защиты в ИС (при их наличии), работниками ОМСУ.

27. Администратор безопасности ИС:

Осуществляет установку и сопровождение САЗ ИС в соответствии с требованиями законодательства Российской Федерации и Московской области в области защиты информации;

Осуществляет периодическое обновление баз вирусных сигнатур САЗ;

Осуществляет внеплановые проверки СВТ в ИС ОМСУ на наличие вредоносного ПО;

Участвует в расследовании инцидентов информационной безопасности, связанных с нарушениями Политики в ИС;

Проводит повседневный контроль действий пользователей ИС в части антивирусной защиты;

Проводит разъяснительную и консультационную работу с пользователями ИС в части в части использования САЗ;

Соблюдает требования законодательства Российской Федерации и Московской области, положения Политики, инструкции по обеспечению антивирусной защиты в ОМСУ, а также инструкций по обеспечению антивирусной защиты в ИС (при их наличии).

28. Специалисты, ответственные за техническое обслуживание ИС:

Осуществляют установку и сопровождение САЗ (в ИС, не предназначенных для обработки ИОД);

Участвуют в расследовании инцидентов, связанных с нарушениями Политики в ОМСУ;

Осуществляют внеплановые проверки СВТ работников ОМСУ на наличие вредоносного ПО;

Проводят разъяснительную и консультационную работу с работниками ОМСУ в части пользования САЗ;

Соблюдают требования законодательства Российской Федерации и Московской области, положения Политики, инструкции по обеспечению антивирусной защиты в ОМСУ, а также инструкций по обеспечению антивирусной защиты в ИС (при их наличии).

29. Работники ОМСУ:

Проводят антивирусный контроль информации (посредством штатных САЗ) всей информации, поступающей на их АРМ по каналам связи или направляемой по каналам связи с указанных АРМ;

При обнаружении вредоносных программ немедленно уведомляют о факте заражения администратора безопасности ИС или лицо, ответственное за защиту информации в ОМСУ либо специалистов, ответственных за техническое обслуживание ИС (в ИС, не предназначенных для обработки ИОД);

Соблюдают требования законодательства Российской Федерации и Московской области, положения Политики, инструкции по обеспечению антивирусной защиты в ОМСУ, а также инструкций по обеспечению антивирусной защиты в ИС (при их наличии).

V. Контроль соблюдения Политики и ответственность за её нарушение

30. Ответственность за исполнение Политики в ОМСУ в ОМСУ возглавляется на руководителя ОМСУ.

31. Повседневный антивирусный контроль ИС и обрабатываемых информационных ресурсов возлагается на пользователей ИС.

32. Периодический контроль соблюдения антивирусной безопасности в ИС возлагается на администратора безопасности ИС либо (в ИС, не предназначенных для обработки ИОД) на специалистов, ответственных за техническое обслуживание ИС.

33. Ответственность за правильность выбора САЗ в ИС возлагается на лицо, ответственное за обеспечение защиты информации в ОМСУ либо (в ИС, не предназначенных для обработки ИОД) на специалистов, ответственных за техническое обслуживание ИС.

34. Ответственность за правильность установки, настройки, эксплуатации САЗ и своевременное обновление баз вирусных сигнатур САЗ возлагается на администратора безопасности ИС либо (в ИС, не предназначенных для обработки ИОД) на специалистов, ответственных за техническое обслуживание ИС.

35. Лица, участвующие в процессах, описанных в Политике, несут ответственность за выполнение возлагаемых на них функциональных обязанностей в соответствии с законодательством Российской Федерации и Московской области.