АДМИНИСТРАЦИЯ
ДМИТРОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
МОСКОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

24.05.2018 № 3613-П

г. Дмитров

Об утверждении политики антивирусной защиты в Администрации Дмитровского муниципального района Московской области

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», распоряжением Министерства государственного управления информационных технологий и связи от 19.07.2017 № 10-86/РВ «Об утверждении политики антивирусной защиты центральных исполнительных органов государственной власти Московской области и государственных органов Московской области» и в целях совершенствования системы защиты информации Администрации Дмитровского муниципального района Московской области:

1. Утвердить прилагаемую политику антивирусной защиты информационных систем Администрации Дмитровского муниципального района Московской области.
2. Рекомендовать руководителям управлений, отделов, секторов Администрации Дмитровского муниципального района Московской области обеспечить защиту информации в соответствии с утвержденной политикой антивирусной защиты.
3. Обеспечить размещение настоящего постановления на официальном сайте Администрации в сети Интернет.
4. Контроль за исполнением настоящего постановления оставляю за собой.

Глава Дмитровского муниципального района Московской области Е.Б. Трошенкова

05.10.15.

АО «Первая Образцовая типография», филиал «Фабрика офсетной печати №2» , г. Дмитров, Заказ №585 Тираж 30000 экз. 1 вид

УТВЕРЖДЕНА
постановлением Администрации Дмитровского муниципального района Московской области
от 24.05.2018 № 3613-П

ПОЛИТИКА
антивирусной защиты информационных систем Администрации Дмитровского муниципального района Московской области

Перечень используемых сокращении

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;

ЦИОГВ и ГО - центральные исполнительные органы государственной власти Московской области и государственные органы Московской области.

I. Общие положения

1.Настоящая Политика антивирусной защиты информационных систем Администрации Дмитровского муниципального района Московской области (далее Политика) определяет состав и порядок мероприятий по антивирусной защите ИС Администрации Дмитровского муниципального района Московской области(далее Администрация) и СВТ работников Администрации.

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 Администрации.

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 №21 «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. Утвержден решением председателя 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 Администрации должны быть разработаны с учетом положений Политики и утверждены Главой Дмитровского муниципального района Московской области инструкции по антивирусной защите информации в ИС Администрации.

7. Требования к осуществлению антивирусной защиты каждой отдельной ИС Администрации должны определяться индивидуально с учетом положений настоящей Политики и должны учитывать особенности технологического процесса обработки информации в этой системе, топологию ИС, а также максимальную разрешенную категорию обрабатываемой информации.

8. Антивирусная защита каждой отдельной ИС Администрации предназначенной для обработки ПДн и (или) иной ИОД либо иной защищаемой информации, обладателями которой является Администрация, должна осуществляться посредством сертифицированных в установленном порядке на соответствие требованиям по безопасности информации САЗ.

9. Требования к осуществлению антивирусной защиты каждой отдельной ИС Администрации 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

12. САЗ должны использоваться во всех сегментах Администрации и на СВТ работников Администрации независимо от наличия в них ИОД.

13. Допускается не применять САЗ на СВТ, не имеющих сетевых подключений, технологический процесс обработки информации которых не предусматривает подключение съемных МНИ и информационного обмена с внешними ИС и СВТ.

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

15. Выбор САЗ для каждой конкретной ИС, указанной в п. 8 Политики, должен производиться ответственным за защиту информации в Администрации 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 в информационных системах Администрации

16. Порядок использования САЗ определяется эксплуатационной документацией конкретного САЗ, инструкцией по антивирусной защите в Администрации, а также инструкцией по антивирусной защите ИС Администрации (при ее наличии).

17. 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.

18. 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 обновление баз вирусных сигнатур САЗ должны осуществляться 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 производиться незамедлительно.

19. При эксплуатации САЗ в Администрации должны выполняться следующие требования:

должна обеспечиваться проверка на отсутствие вредоносного ПО всей поступающей в ИС информации, как по каналам связи (в том числе по электронной почте), так и на съемных МНИ;

должна производиться периодическая проверка несъемных МНИ на отсутствие вредоносного ПО;

антивирусный контроль в ИС должен осуществляться постоянно в автоматическом режиме.

20. В случаях:

выявления факта заражения ресурсов ИС;

подозрения на заражение ресурсов ИС вредоносным ПО;

получения предупреждения о повышенной вирусной активности;

соответствующего поручения Мингосуправления Московской области,

должна производиться внеплановая проверка ИС Администрации и СВТ работников Администрации на отсутствие вредоносного ПО.

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

22. При обнаружении вредоносного ПО пользователь обязан доложить о факте заражения СВТ администратору безопасности ИС или лицу, ответственному за защиту информации Администрации, либо, в ИС, не предназначенных для обработки ИОД - специалистам, ответственным за техническое обслуживание ИС, после чего ими должны быть приняты меры по антивирусной защите, восстановлению поврежденных файлов и восстановлению работоспособности ИС. Информация об инциденте должна быть доведена до Главы Дмитровского муниципального района Московской области в установленном порядке.

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

24. 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.

25. При обнаружении вредоносного ПО в информации, поступившей по каналам связи или со съемных МНИ из ЦИОГВ и ГО либо иных организаций, необходимо сообщить об этом факте лицу, ответственному за защиту информации в Администрации.

IV. Реализация Политики в Администрации

26. Реализация Политики в Администрации осуществляется за счет согласованных действий Главы Дмитровского муниципального района, лиц, ответственных за защиту информации в Администрации, администраторов безопасности ИС, специалистов, ответственных за техническое обслуживание ИС, а также работников Администрации.

27. Глава Дмитровского муниципального района:

назначает ответственного (ответственных) за обеспечение защиты информации в Администрации соответствующим Распоряжением;

назначает администраторов безопасности ИС Администрации соответствующими Распоряжениями (при необходимости);

утверждает инструкцию по обеспечению антивирусной защиты информации в Администрации;

утверждает инструкции по обеспечению антивирусной защиты информации в ИС Администрации (при необходимости);

осуществляет контроль за исполнением Политики в Администрации;

организует расследования инцидентов, связанных с нарушениями Политики в Администрации;

устанавливает ответственность работников Администрации за нарушение Политики;

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

28. Ответственный за обеспечение защиты информации в Администрации:

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 Администрации в части антивирусной защиты информации;

проводит сбор и анализ информации об инцидентах информационной безопасности, связанных с нарушениями Политики в Администрации;

проводит расследование инцидентов, связанных с нарушениями Политики в Администрации;

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

29. 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 Администрации 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 использования САЗ;

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

30. Специалисты, ответственные за техническое обслуживание ИС:

осуществляют установку и сопровождение САЗ в ИС, не предназначенных для обработки ИОД;

осуществляют периодическое обновление баз вирусных сигнатур САЗ в ИС, не предназначенных для обработки ИОД;

участвуют в расследовании инцидентов, связанных с нарушениями Политики в Администрации;

осуществляют внеплановые проверки СВТ работников Администрации на наличие вредоносного ПО;

проводят разъяснительную и консультационную работу с работниками Администрации в части пользования САЗ;

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

31. Работники Администрации:

проводят антивирусный контроль информации (посредством штатных САЗ), обрабатываемой и хранящейся на их СВТ и МНИ (в случае, если антивирусный контроль не проводится в автоматическом режиме);

проводят антивирусный контроль (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 Администрации либо, в ИС, не предназначенных для обработки ИОД - специалистов, ответственных за техническое обслуживание ИС;

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

V. Контроль соблюдения Политики и ответственность за ее нарушение

32. Ответственность за исполнение Политики в Администрации возлагается на Главу Дмитровского муниципального района.

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

34. 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.

35. Ответственность за правильность выбора САЗ в ИС возлагается на лицо, ответственное за обеспечение защиты информации в Администрации либо, в ИС, не предназначенных для обработки ИОД - на специалистов, ответственных за техническое обслуживание ИС.

36. 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 обязанностей в соответствии с законодательством Российской Федерации и Московской области.