emblem

**УПРАВЛЕНИЕ ПО ОБЕСПЕЧЕНИЮ ДЕЯТЕЛЬНОСТИ**

**МИРОВЫХ СУДЕЙ НОВОСИБИРСКОЙ ОБЛАСТИ**

**ПРИКАЗ**

«\_\_\_» \_\_\_\_\_\_\_\_ 2017г. № \_\_\_\_\_

г. Новосибирск

**Об утверждении инструкции по организации антивирусной защиты в АС управления по обеспечению деятельности мировых судей Новосибирской области**

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» в целях реализации постановления Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, **п р и к а з ы в а ю :**

1. Утвердить инструкцию по организации антивирусной защиты в АС управления по обеспечению деятельности мировых судей Новосибирской области (Приложение №1).

2. Контроль за исполнением приказа оставляю за собой.

|  |  |
| --- | --- |
| Начальник управления | В.А. Чиркунов |

ПРИЛОЖЕНИЕ № 1

УТВЕРЖДЕНО

приказом начальника управления по обеспечению деятельности мировых судей

Новосибирской области

от «\_\_\_\_»\_\_\_\_\_2017 №\_\_

**Инструкции по организации антивирусной защиты в АС**

**управления по обеспечению деятельности мировых судей Новосибирской области**

Настоящая Инструкция определяет требования к организации защиты АС управления по обеспечению деятельности мировых судей Новосибирской области (далее - Управление):

от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников Управления, эксплуатирующих и сопровождающих АС Управления, за их выполнение.

К использованию в Управлении допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению.

В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с начальником Управления.

Установка средств антивирусного контроля на компьютерах (серверах ЛВС АС Управления) и настройка параметров средств антивирусного контроля осуществляется уполномоченными сотрудниками отдела материально-технического обеспечения Управления.

**Применение средств антивирусного контроля**

Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов РС.

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 (магнитных дисках, лентах, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании соответствующего нормативного акта управления. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено сотрудником отдела материально-технического обеспечения Управления на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка:

- на защищаемых серверах и РС - ответственным за обеспечение информационной безопасности;

- на других серверах и РС АС управления не требующих защиты, - лицом, установившим (изменившим) программное обеспечение.

Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале подразделения за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

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 Управления самостоятельно или вместе с ответственным за обеспечение безопасности информации сотрудником должен провести внеочередной антивирусный контроль своей рабочей станции. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники Управления обязаны:

* приостановить работу;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за обеспечение информационной безопасности Управления, владельца зараженных файлов, а также смежные отделы, использующие эти файлы в работе;
* 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 специалистов отдела);
* в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на гибком магнитном диске в отдел для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при необходимости, для выполнения требований данного пункта привлечь специалистов отдела материально-технического обеспечения Управления);
* 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, тип вируса и выполненные антивирусные мероприятия.

**Ответственность**

Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем АС Управления, в соответствии с требованиями настоящей Инструкции возлагается на начальника соответствующего отдела.

Ответственность за проведение мероприятий антивирусного контроля в Управлении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности информации и всех сотрудников Управления, являющихся пользователями АС Управления.