|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | УТВЕРЖДаЮ | |
|  | | | Директор ООО «» | |
|  | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_ | |
|  | | | «\_\_\_» \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_ г. | |
|  |  | | |
| **ИНСТРУКЦИЯ**  **по антивирусной защите**  **в ООО «»** | | | |
|  | | | |
|  | |  | |
|  | |  | |
|  | |  | |
|  | |  | |
|  | |  | |
|  | |  | |
|  | |  | |

1. **Область применения**
   1. Настоящая инструкция определяет требования к организации защиты автоматизированных систем от разрушающего воздействия компьютерных вирусов, вредоносных программ, исполняемых кодов и устанавливает ответственность пользователей автоматизированной системы за их выполнение.
   2. Настоящая инструкция разработана на основании и в соответствии с нормативно-методическими документами и нормативно-правовыми актами Российской Федерации в области обеспечения безопасности информации и является дополнением к действующим нормативным документам, определяющим порядок соблюдения требований по защите персональных данных и информационной безопасности в ООО «».
2. **Термины и определения**
   1. В настоящей инструкции применены следующие термины с соответствующими определениями:
      1. **аттестованная автоматизированная система**: Автоматизированная система, на которой проведены работы по аттестации на соответствие требованиям по безопасности информации (по линии Федеральной службы по техническому и экспортному контролю Российской Федерации) и имеется действующий аттестат соответствия.
      2. **вирус**: Разновидность компьютерных программ, отличительной особенностью которых является способность к размножению (саморепликации) и классифицирующиеся по воздействию на автоматизированные системы:

* по поражаемым объектам (файловые вирусы, загрузочные вирусы, скриптовые вирусы, макровирусы, вирусы, поражающие исходный код);
* по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);
* по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
* по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, скриптовый язык и др.);
* по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

1. **Обозначения и сокращения**

В настоящей инструкции применены следующие обозначения и сокращения:

АВЗ– антивирусная защита

АРМ – автоматизированное рабочее место

АС – автоматизированная система

ИСПДн – информационная система персональных данных

ЛВС – локальная вычислительная сеть

ОСА – отдел системного администрирования

ПДн – персональные данные;

ПО – программное обеспечение

ОИБ – отдел информационной безопасности

УИТ – управление информационных технологий

ФСТЭК РФ – Федеральная служба по техническому и экспортному контролю Российской Федерации

1. **Общие положения**
   1. К использованию в АС ООО «» допускаются только лицензионные антивирусные средства. Для использования в АС и ИСПДн, прошедших процедуру аттестации или оценки эффективности мер по обеспечению безопасности ПДн антивирусные средства должны иметь сертификат соответствия требованиям по безопасности.
   2. Передача средств антивирусной защиты на объекты, не входящие в состав ООО «», запрещена. За несанкционированное распространение средств антивирусной защиты виновные несут ответственность в соответствии с действующим законодательством Российской Федерации.
   3. Все АС и ИСПДн ООО «», входящие в состав ЛВС, подлежат обязательному оснащению средствами АВЗ.
   4. Практическое выполнение мероприятий по организации антивирусной защиты в АС и ИСПДн возлагается на администратора АС и ИСПДн.
   5. В аттестованных системах функции администратора антивирусной защиты полностью или частично могут быть возложены на иное лицо в соответствии с технологическим процессом обработки информации.
   6. Своевременную инсталляцию средств антивирусной защиты информации и обновление баз данных вирусных описаний, а также настройку параметров защиты средств АВЗ осуществляет администратор автоматизированных систем и информационной системы персональных данных. Самостоятельная установка, обновление и настройка ПО АВЗ пользователями АС не допускается.
   7. Установка и настройка параметров защиты средств АВЗ на АРМ пользователей, осуществляется в соответствии с программной и эксплуатационной документацией на средства АВЗ.
2. **Применение средств антивирусного контроля**
   1. Регулярно при каждой загрузке АРМов, входящих в состав АС или ИСПДн, в автоматическом режиме должен загружаться монитор АВЗ – резидентный (постоянно находящийся в оперативной памяти АС) модуль проверки файлов.
   2. Обязательному входному антивирусному контролю подлежат поступающие в АС и ИСПДн программные средства, любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Обязательная проверка используемых в работе съемных носителей должна осуществляться перед началом работы с ними. Контроль исходящей информации необходимо проводить непосредственно перед ее отправкой (записью на съемный носитель).
   3. Ввод новых АРМ с предустановленным ПО в эксплуатацию, а также включение их в состав других АС и ИСПДн осуществляется после проведения полного антивирусного контроля.
   4. Для сохранности информации ограниченного распространения необходимо проведение регулярных мероприятий по архивированию (резервному копированию), для возможности восстановления информации при поражении АС и ИСПДн вредоносным ПО. Файлы, помещаемые в электронный архив, должны проходить антивирусный контроль перед архивированием. Проверка электронных архивов проводится антивирусной программой автоматически. Реализация указанных мероприятий возлагается на работников ООО «» в соответствии с технологическим процессом обработки информации.
   5. Обновление антивирусных баз средств антивирусной защиты, используемых для защиты АС, может осуществляться:

* централизованно администратором АС и ИСПДн без участия пользователей посредством механизма централизованного управления и обновления антивирусных баз;
* путем ручного копирования антивирусных баз администратором АС и ИСПДн непосредственно в АРМ, не подключенные к ЛВС.
  1. В качестве источника обновления антивирусных баз должны выступать сервер АВЗ. Обновление баз данных вирусных описаний должно осуществляться не реже одного раза в неделю.
  2. При появлении сообщений АВЗ об отсутствии обновления антивирусных баз более чем недельной давности, а также о любых других ошибках в работе АВЗ, пользователь обязан приостановить работу и немедленно уведомить администратора АС и ИСПДн и администратора безопасности АС и ИСПДн.
  3. Для аттестованных АС периодическая проверка жестких магнитных дисков АС на отсутствие вирусов должна проводиться непосредственно пользователями АС вручную или по расписанию не реже одного раза в месяц, после проведения обновления баз данных вирусных описаний. Периодическая проверка серверов в аттестованных АС осуществляется администраторами АС и ИСПДн не реже одного раза в месяц после проведения обновления антивирусных баз. Для аттестованных АС проверка также проводится при каждом изменении состава ПО АС и ИСПДн.
  4. Внеплановая проверка жестких магнитных дисков АС и ИСПДн на отсутствие вирусов должна проводиться при подозрении на наличие в АС и ИСПДн вирусов. Перед внеплановой проверкой обязательно проведение обновления антивирусных баз.
  5. Для проведения проверки жестких магнитных дисков АС и ИСПДн на отсутствие вирусов допускается использовать тестовые программы-вирусы, полученные от производителя. Обнаружение АВЗ тестовых программ-вирусов не является фактом обнаружения вируса и свидетельствует о правильной работе ПО АВЗ.
  6. 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 АС самостоятельно или совместно с администратором АС и ИСПДн должен провести внеплановую проверку на отсутствие программных вирусов.
  7. Факт выполнения антивирусной проверки для аттестованных АС должен регистрироваться в журнале антивирусных проверок АС подразделения за подписью лица, проводившего проверку.

Форма журнала антивирусных проверок АС приведена в приложении А.

Журнал антивирусных проверок находится у администратора АС и ИСПДн и заполняется администратором АС и ИСПДн при проведении проверки зараженных файлов.

1. **Действия при обнаружении вирусов**
   1. При обнаружении зараженных компьютерными вирусами файлов пользователи обязаны:

* остановить работу;
* о факте обнаружения зараженных вирусом файлов немедленно поставить в известность администратора АС и ИСПДн, администратора безопасности АС и ИСПДн, руководителя подразделения;
* совместно с администратором АС и ИСПДн провести анализ необходимости дальнейшего использования зараженных файлов, по возможности провести лечение зараженного файла;
* в случае невозможности вылечить зараженный файл, необходимо поместить его в карантин, и выполнить процедуру по восстановлению незараженной копии исходного файла из имеющегося архива;
* в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, решение о дальнейших действиях с зараженными файлами принимает администратор АС и ИСПДн;
* для аттестованных АС сделать запись в журнале антивирусных проверок АС и ИСПДн, а также оформить служебную записку на имя директора ООО «» по факту обнаружения зараженных вирусом файлов, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, наименование вируса и выполненные антивирусные мероприятия.
  1. Возобновление обработки информации на АРМ, входящих в состав АС и ИСПДн, после заражения АРМ вирусом возможно только после полной проверки АРМ на отсутствие вирусов с проведенным обновлением антивирусных баз.
  2. При повреждении программных средств и информационных массивов компьютерными вирусами должны выполняться мероприятия по восстановлению их работоспособности.

1. **Ответственность**
   1. Непосредственное руководство проведением работ по антивирусной защите информации в ООО «» осуществляют ответственный за обеспечение безопасности персональных данных в ООО «».
   2. Ответственность за выполнение мероприятий антивирусной защиты в подразделениях ООО «» и соблюдение требований настоящей инструкции возлагается на руководителей структурных подразделений.
   3. Непосредственную ответственность за соблюдение установленных норм обеспечения антивирусной защиты при работе в АРМ, входящих в состав АС и ИСПДн, несут пользователи АС.
2. **Контроль**

Контроль за состоянием антивирусной защиты в АС и ИСПДн ООО «», а также за соблюдением установленного порядка антивирусной защиты и выполнением требований настоящей инструкции пользователями, осуществляет ответственный за обеспечение безопасности персональных данных в ООО «».

**Приложение А**

(рекомендуемое)

**Форма журнала антивирусных проверок АС**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Журнал антивирусных проверок АС**   | № п/п | Дата и время проверки | Наименование АС (составной части АС) | Какими средствами проводилась проверка | Результаты проверки | | Наименование инфицированных файлов, источника поступления (носитель, организация) | Примечание (принятые меры) | Фамилия и подпись лица, проводившего проверку | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Кол-во проверенных файлов | Кол-во инфициро-ванных файлов | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |