

«19» сентября 2023 г.

ИНСТРУКЦИЯ
по организации антивирусной защиты информационных систем персональных данных в
ООО «Институт конструктивной психологии»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция по организации антивирусной защиты информационных систем персональных данных в организации определяет требования к организации защиты информационных систем персональных данных (далее ИСПДн) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (ПО) и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. Требования настоящей Инструкции обязательны для всех должностных лиц и сотрудников организации, использующих в работе ИСПДн организации, а также всех пользователей СВТ.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, Ответственным за ИСПДн проводятся организуемые семинары и персональные инструктажи (при необходимости) пользователей ИСПДн.

1. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

1.1. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

1.2. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).

1.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD(DVD)-ROM и флеш-накопителях т.п.).

1.4. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема.

1.5. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

1.6. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

2. ФУНКЦИИ ОТВЕТСТВЕННОГО ЗА ИСПДН ПО ОБЕСПЕЧЕНИЮ АНТИВИРУСНОЙ БЕЗОПАСНОСТИ

Ответственный за ИСПДн обязан:

- 2.1. При необходимости проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты.
- 2.2. Настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.
- 2.3. Предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов.
- 2.4. При необходимости производить обновление антивирусных программных средств или настраивать систему автоматического обновления.
- 2.5. Производить получение и рассылку обновлений антивирусных баз (при необходимости).
- 2.6. Разрабатывать инструкции по работе пользователей с программными средствами антивирусной защиты (при необходимости).
- 2.7. Проводить работы по обнаружению и обезвреживанию вирусов.
- 2.8. Участвовать в работе комиссии по расследованию причин заражения ПЭВМ и серверов.
- 2.9. Осуществлять периодический контроль соблюдения пользователями ПЭВМ требований настоящей Инструкции;

3. ФУНКЦИИ ПОЛЬЗОВАТЕЛЕЙ

Пользователи ИСПДн в особенности и остальные пользователи СВТ:

- 3.1. 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.) сотрудник самостоятельно или вместе с ответственным за ИСПДн должен провести внеочередной антивирусный контроль ПЭВМ.
- 3.2. В случае обнаружения (подтверждения факта наличия вируса) при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:
 - 4.1.1. приостановить работу;
 - 4.1.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя организации и ответственного за ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
 - 4.1.3. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
 - 4.1.4. провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за ИСПДн);
 - 4.1.5. в случае обнаружения вируса, не поддающегося лечению установленными антивирусными средствами, передать зараженный вирусом файл на съемном носителе ответственного за ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;
 - 4.1.6. по факту обнаружения зараженных вирусом файлов составить служебную записку ответственному за ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

4. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

- 4.1. Инструкция подлежит полному пересмотру в случае приобретения организацией новых средств защиты, существенно изменяющих порядок работы с ними.
- 4.2. В остальных случаях Инструкция подлежит частичному пересмотру.

4.3. Полный пересмотр данной Инструкции проводится с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн организации.

5. КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

5.1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников Организации.

5.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам антивирусной защиты возлагается на ответственного за ИСПДн.

Ведомость ознакомления

№ п/п	Фамилия И.О. сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении