Приложение №2
к приказу от «25» 03 2025 № 65/02

УТВЕРЖДАЮ
Врио директора
ФГБУ «СибНИГМИ»
В.Н. Копылов
«25» 03 2025 г.

Инструкция
по проведению антивирусного контроля и антивирусной защиты в информационных системах персональных данных ФГБУ «СибНИГМИ»

1. Общие положения

Настоящая Инструкция определяет требования к организации программного обеспечения (далее – ПО), участвующего в обработке персональных данных от разрушающего воздействия компьютерных вирусов и иного вредоносного ПО, и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих информационные системы персональных данных (далее – ИСПДн), за их выполнение.

2. Установка и обновление антивирусных средств

2.1. На рабочих местах ИСПДн может использоваться программное и аппаратное обеспечение, необходимое только для выполнения служебной деятельности и согласованное с отделом информационных технологий и автоматизации управления (ИТиА).

2.2. Запрещается использовать на автоматизированных рабочих местах (далее – АРМ), участвующих в обработке защищаемой информации, программные и аппаратные средства, не согласованные с регламентирующими документами ФСТЭК и ФСБ.

2.3. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, имеющие соответствующий сертификат ФСТЭК по защите персональных данных.

2.4. Установка средств антивирусного контроля на АРМ и серверах ИСПДн осуществляется Администратором ИСПДн в соответствии с Инструкцией по установке и эксплуатации производителя соответствующего средства антивирусного контроля. Настройка параметров средств антивирусного контроля осуществляется Администратором ИСПДн в соответствии Инструкцией по установке и эксплуатации соответствующего средства антивирусного контроля и принятой в управлении политикой антивирусного контроля.

2.5. Регулярное обновление антивирусных средств осуществляется автоматически и контролируется Администратором безопасности ИСПДн, ответственными за организацию антивирусной защиты. В случае получения пользователем на рабочем месте сообщения о невозможности (сбое) автоматического обновления, необходимо оповестить об этом Администратора безопасности ИСПДн.

3. Применение средств антивирусного контроля

3.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль системной памяти, объектов автозапуска и загрузочных секторов всех дисков компьютера.

3.2. Полная антивирусная проверка компьютера должна включать проверку всех жестких дисков, всех сменных дисков и устройств, почтовых ящиков, резервного хранилища системы.

Она должна проводиться регулярно, не реже одного раза в месяц и может регламентироваться и контролироваться сервером администрирования антивирусной защиты ИСПДн.

3.3. Обязательному постоянному 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, запоминающих устройств USB, 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).

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

3.5. Установка (изменение) системного и прикладного ПО осуществляется на основании инструкции по установке и эксплуатации ПО и аппаратных средств ИСПДн производителя данного. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено отделом ИТиА на отсутствие вирусов. Непосредственно после установки (изменения) ПО АРМ и/или серверах ИСПДн, должна быть выполнена антивирусная проверка:

- на защищаемых серверах - Администратором безопасности ИСПДн;
- на АРМ – Администратором ИСПДн;
- на других серверах и рабочих станциях, не требующих защиты, - лицом, установившим (изменившим) ПО, - в присутствии и под контролем Администратора ИСПДн.

3.6. Факт выполнения полной антивирусной проверки после установки (изменения) ПО должен регистрироваться в специальном журнале (электронном).

3.7. 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 подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации подразделения (технологического участка) должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь Администратора ИСПДн для определения им факта наличия или отсутствия компьютерного вируса.

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора безопасности ИСПДн, владельца зараженных файлов, а также смежные подразделения, 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 Администратором ИСПДн);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, Администратора безопасности ИСПДн должен передать его в организацию, с которой заключен договор на антивирусную поддержку (разработчику антивирусного ПО);
- по факту обнаружения зараженных вирусом файлов составить служебную записку в

отдел ИТиА Администратору безопасности ИСПДн, 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.

5. Ответственность при организации антивирусной защиты

5.1. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на ответственного по защите персональных данных в информационных системах.

5.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на ответственного по защите персональных данных в информационных системах.

5.3. Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками управлении осуществляется ответственным по защите персональных данных в информационных системах.