УТВЕРЖДАЮ

Директор ГБОУ СО «Верхнесинячихинская школа-интернат»

\_\_\_\_\_\_\_\_\_\_\_\_\_ О.А. Бурухина

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.

Регламент по организации резервного копирования в информационных системах персональных данных ГБОУ СО «Верхнесинячихинская   
школа-интернат»

# Общие положения

Настоящий регламент разработан в соответствии с требованиями Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных», Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 г. № 21   
«Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также прочих нормативных документов по защите информации.

Настоящий регламент определяет порядок резервирования и восстановления работоспособности технических средств (далее – ТС) и программного обеспечения (далее – ПО), баз данных, средств защиты информации и определяет действия, связанные с функционированием информационных систем персональных данных ГБОУ СО «Верхнесинячихинская школа-интернат» (далее – ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Действие настоящего регламента распространяется на всех пользователей ИСПДн, имеющих доступ к ее ресурсам, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе: системы жизнеобеспечения; системы обеспечения отказоустойчивости; системы резервного копирования и хранения данных; системы контроля физического доступа.

# Меры обеспечения непрерывности работы и восстановления ресурсов

## Технические меры.

К техническим мерам обеспечения непрерывной работы и восстановления относятся системы обеспечения отказоустойчивости и системы резервного копирования и хранения данных.

Все критичные помещения ГБОУ СО «Верхнесинячихинская школа-интернат» (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и (или) средствами пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны, по возможности, применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания (или встроенные аккумуляторы).

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на отчуждаемый носитель (внешний жесткий диск, флеш-диск и т.д.).

## Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе ‑ для обрабатываемых персональных данных – не реже раза в неделю; для технологической информации – не реже раза в месяц; эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведении процедуры резервного копирования, рекомендуется отражать в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы и учтены: номером носителя, датой проведения резервного копирования. Данные носители необходимо учитывать в «Журнале учета и выдачи машинных носителей информации, используемых в информационных системах персональных данных ГБОУ СО «Верхнесинячихинская школа-интернат».

Носители должны храниться в запираемом шкафу, сейфе, или любом другом месте хранения с ограниченным доступом, в помещении, оборудованном системой охранно-пожарной сигнализации.

Носители должны храниться не менее года, для возможности восстановления данных.

# Ответственность

Организационное и техническое обеспечение процессов резервного копирования и восстановления информации во всех ИСПДн возлагается на администратора безопасности.

Ответственность за соблюдение требований настоящего регламента возлагается на всех сотрудников, являющихся пользователями ИСПДн.

Нарушение требований настоящего регламента влечет за собой ответственность, предусмотренную законодательством Российской Федерации.

**РАЗРАБОТАНО:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ответственный за организацию обработки и обеспечение безопасности персональных данных |  |  |  | А.Е. Запольских |
|  |  | (подпись, дата) |  | (инициалы, фамилия) |

**С документом ознакомлен (а):**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Директор |  |  |  | О.А. Бурухина |
|  |  | (подпись, дата) |  | (инициалы, фамилия) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Администратор безопасности ИСПДн |  |  |  |  | Н.А. Блохин |
|  |  |  | (подпись, дата) |  | (инициалы, фамилия) |

Приложение №1

**Лист ознакомления с регламентом**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Ф.И.О.**  **работника** | **Личная подпись** | **Дата ознакомления** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |