**СОГЛАСОВАНО**

**Председатель профкома**

**_____ О.М. Баландина**

**« ___ » _____ 2018 г.**

**УТВЕРЖДАЮ**

**– Директор МОУ-СОШ №1**

**–**

**_____ Л.П. Карманова**

**« ___ » _____ 2018 г.**


Подписан: Карманова Лидия Прокопьевна
DN: C=RU, O=МОУ-СОШ №1 г. Петровск-Забайкальский, CN=Карманова Лидия Прокопьевна, E=school-1-pzb@mail.ru
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: г. Петровск-Забайкальский
Дата: 2022.04.15 12:00:33+09'00'

# ПОЛОЖЕНИЕ О РЕЖИМЕ БЕЗОПАСНОСТИ В ПОМЕЩЕНИЯХ

## предназначенных для обработки персональных данных в МОУ-СОШ №1

**2018 г.**

## 1. Общие положения

1.1. Настоящее Положение устанавливает организацию и порядок обеспечения режима безопасности в помещениях МОУ-СОШ №1, в которых размещаются технические средства, предназначенные для обработки персональных данных в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение разработано на основе действующих в Российской Федерации правовых и нормативных документов по защите информации.

1.3. Режим безопасности в помещениях ИСПДн обеспечивается следующими методами и способами защиты информации от несанкционированного доступа:

- Реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанной с ее использованием работам, документам;
- Ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;
- Размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории.
- Организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных.

## 2. Общие требования по физической защите объекта информатизации

2.1. Эксплуатация ИСПДн и системы защиты информации в ее составе должна осуществляться в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией.

2.2. С целью предотвращения либо существенного затруднения проникновения в здания, помещения посторонних лиц, хищения технических средств, документов и носителей информации должна быть организована физическая защита помещений и собственно технических средств обработки информации с использованием технических средств охраны.

2.3. Должно быть организовано ограничение доступа персонала в помещения, где размещено коммутационное и серверное оборудование.

2.4. На период обработки защищаемой информации в помещениях, где размещаются средства обработки информации, могут находиться только лица, допущенные к обрабатываемой информации в установленном порядке.

2.5. Допуск в эти помещения других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться только с санкции руководителя учреждения или руководителя подразделения, эксплуатирующего ИСПДн, по согласованию с администратором информационной безопасности ИСПДн. При этом должны быть соблюдены меры, исключающие ознакомление этих лиц с конфиденциальной информацией. Рекомендуется обеспечивать защиту таких помещений соответствующими средствами контроля доступа.

2.6. С целью исключения предоставления избыточных прав доступа к информации в процессе эксплуатации ИСПДн должен осуществляться периодический пересмотр прав доступа пользователей к информации.

2.7. В случае размещения в одном помещении различных технических средств одной или нескольких ИСПДн должен быть исключен несанкционированный просмотр конфиденциальной информации.

2.8. Учет, хранение и обращение с накопителями и носителями информации на бумажной, магнитной, оптической и иной основе должны осуществляться в соответствии с требованиями Руководящих документов ФСТЭК России и в соответствии с выбранным классом защищенности информационной системы.

2.9. Обращение с ключевыми документами средств криптографической защиты информации (СКЗИ), в случае их использования, должно осуществляться в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

2.10. При увольнении или изменении должностных обязанностей пользователей и администраторов ИСПДн, в установленном в организации порядке должны быть приняты меры по оперативному изменению соответствующих паролей и прав доступа.

2.11. Контроль состояния и эффективности защиты информации осуществляется администратором информационной безопасности ИСПДн и заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер, в проверке выполнения норм эффективности защиты информации ограниченного доступа в соответствии требованиями нормативных документов по защите информации.

## 3. Порядок охраны и допуска посторонних лиц в защищаемые помещения

3.1. Вскрытие и закрытие помещений осуществляется работниками, работающими в данных помещениях. Список служащих, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается руководителем и передаётся на пост охраны.

3.2. При отсутствии служащих, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа, о чем составляется акт.

3.3. При закрытии помещений и сдачей их под охрану служащие, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержится конфиденциальная информация убираются для хранения в опечатываемый сейф (металлический шкаф).

3.4. При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и (или) администратору информационной безопасности. Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.

3.5. Руководитель, ответственный за защиту информации и администратор информационной безопасности организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

3.6. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или руководителю, или администратору информационной безопасности. Помещения вскрывать запрещается.

3.7. Помещения вскрываются ответственным за помещение, или руководителем, в присутствии сотрудника охраны с составлением акта.

3.8. В соответствии с требованиями данного Положения при обработке защищаемой информации в ИСПДн необходимо исключить не контролируемое пребывание посторонних лиц в пределах границ контролируемой зоны ИСПДн, определенных соответствующим приказом.