

**УТВЕРЖДАЮ**

Директор МБОУ СОШ №26

 Н.А.Шишкин

«12» сентября 2018 г.

**Регламент  
доступа в помещения с компонентами информационных систем персональных  
данных и на территорию МБОУ СОШ №26**

**г.Ставрополь  
2018 г.**

## СПИСОК СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
СВТ	Средства вычислительной техники
СЗПДн	Система защиты персональных данных

**СОДЕРЖАНИЕ**

1.	ОБЩИЕ ПОЛОЖЕНИЯ.....	4
2.	ПОРЯДОК ПРОПУСКА (ПРОХОДА) ЛИЦ НА ТЕРРИТОРИЮ ОРГАНИЗАЦИИ.....	4
3.	ВНОС(ВВОЗ) И ВЫНОС (ВЫВОЗ) МАТЕРИАЛЬНЫХ ЦЕННОСТЕЙ .....	5
4.	ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПОМЕЩЕНИЙ .....	5
5.	РЕЖИМ ДОСТУПА В ПОМЕЩЕНИЯ.....	6
6.	РЕЖИМ ПРИ ОБСЛУЖИВАНИИ И РЕМОНТЕ В ПОМЕЩЕНИИ .....	7
7.	СМЕНА КОДОВ И КЛЮЧЕЙ.....	7
8.	ПОРЯДОК ПЕРЕСМОТРА РЕГЛАМЕНТА.....	8
9.	ОТВЕТСТВЕННЫЕ ЗА ВЫПОЛНЕНИЕ РЕГЛАМЕНТА.....	8
	ПРИЛОЖЕНИЕ 1 ФОРМА СПИСКА СОТРУДНИКОВ .....	10
	ПРИЛОЖЕНИЕ 2 ФОРМА РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РЕГЛАМЕНТЕ .....	11
	ПРИЛОЖЕНИЕ 3 ПЕРЕЧЕНЬ ПОМЕЩЕНИЙ ДЛЯ РАЗМЕЩЕНИЯ ИСПДН.....	12

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящий регламент определяет порядок доступа в помещения, в которых располагаются компоненты (АРМ, серверы, сетевое оборудование и т.п.) информационных систем персональных данных (ИСПДн) и на территорию МБОУ СОШ № 26 города Ставрополя (далее Учреждение).
- 1.2. Выполнение требований настоящего Регламента обязательно для всех сотрудников Учреждения, осуществляющих свою деятельность на территории Учреждения.
- 1.3. В целях закрепления знаний по вопросам практического исполнения требований Регламента, разъяснения возникающих вопросов Администратор ИБ ИСПДн проводятся семинары (не реже 1 раз в год) и/или персональные инструктажи (при необходимости) сотрудников.
- 1.4. Настоящий Регламент не определяет режимные меры в нештатных ситуациях требующих немедленной эвакуации из помещений персонала, документации, средств вычислительной техники (СВТ) и т.д, таких как:
  - пожар,
  - наводнение,
  - землетрясение, и др.
- 1.5. В случае невозможности исполнения требований настоящего Регламента в полном объеме, например:
  - в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок в работе ИСПДн, стихийных бедствий, побочных влияний;
  - злоумышленных действий.
- 1.6. Ознакомление с требованиями Регламента администраторов информационной безопасности проводит ответственный за безопасность под роспись с выдачей электронных копий соответствующих приложений и разделов Регламента непосредственно для повседневного использования в работе.
- 1.7. Ознакомление начальников отделов Организации с требованиями Регламента проводит Администратор ИБ ИСПДн под роспись с выдачей электронных копий Регламента непосредственно для повседневного использования в работе.
- 1.8. Ознакомление сотрудников Организации с требованиями Регламента проводят начальники этих отделов под роспись с выдачей электронных копий Регламента непосредственно для повседневного использования в работе.

Практическая «глубина» исполнения настоящего Регламента может оперативно определяться Администратором ИБ ИСПДн по согласованию с ответственным за защиту ПДн.

## 2. ПОРЯДОК ПРОПУСКА (ПРОХОДА) ЛИЦ НА ТЕРРИТОРИЮ ОРГАНИЗАЦИИ

- 2.1. Доступ сотрудников на территорию Учреждения осуществляется по предъявлению удостоверения.
- 2.2. Доступ посетителей в вестибюль в рабочее время осуществляется в свободном режиме.
- 2.3. Порядок доступа в помещения с компонентами ИСПДн определен в разделе 5 настоящего документа.
- 2.4. Доступ сотрудников на территорию и во внутренние помещения Учреждения в нерабочее время осуществляется только по согласованию с начальником управления образования, а в помещения с компонентами ИСПДн – по согласованию с начальником управления образования и ответственным за защиту ПДн.
- 2.5. Запрещен проход на территорию Учреждения лиц в состоянии алкогольного, наркотического или иного токсического опьянения.
- 2.6. О попытках несанкционированного входа на территорию и во внутренние помещения Учреждения, а так же о несанкционированном нахождении лиц на территории и во внутренних помещениях Учреждения сотрудник докладывает своему непосредственному начальнику, а о несанкционированном входе сотрудников или иных лиц в помещения с компонентами с ИСПДн и/или нахождения в помещениях с компонентами с ИСПДн докладывает также и ответственному за защиту ПДн.

### **3. ВНОС(ВВОЗ) И ВЫНОС (ВЫВОЗ) МАТЕРИАЛЬНЫХ ЦЕННОСТЕЙ**

- 3.1. На территорию компании запрещается вносить(ввозить):
  - хозяйственные сумки, чемоданы, свертки и компьютеры без соответствующего разрешения;
  - взрывчатые вещества;
  - горючие и легковоспламеняющиеся жидкости и материалы;
  - алкогольную продукцию, наркотические и психотропные вещества.
- 3.2. Запрещается несанкционированный вынос (вывоз) или несанкционированное перемещение материальных ценностей Учреждения.
- 3.3. Запрещается вынос (вывоз) документов, электронных или иных носителей ПДн, а также их передача лицам, не допущенным к обработке ПДн, без согласования с Администратором ИБ ИСПДн или ответственным за защиту ПДн Учреждения.

### **4. ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПОМЕЩЕНИЙ**

- 4.1. Помещения с компонентами ИСПДн (далее - Помещения) оборудуются:
  - надежными механическими замками (минимум - с двумя комплектами ключей);
  - устройствами для опечатывания дверей Помещения;
  - списками сотрудников, имеющих право самостоятельно находиться в Помещении (далее Списки).

- 4.2. Кроме того, желательно оборудование помещений с серверным, сетевым оборудованием, оборудованием подсистемы межсетевого экранирования ИСПДн кодовыми электромеханическими замками или другими средствами разграничения и/или контроля доступа.
- 4.3. Один комплект ключей используется подразделением в постоянной работе, второй комплект, сдается начальнику отдела.
- 4.4. Списки составляет Администратор ИБ ИСПДн и утверждает руководитель подразделения по форме в Приложении 1 к настоящему Регламенту. В данные Списки вносятся только те сотрудники, право самостоятельного нахождения в Помещении которых обусловлено производственной необходимостью.
- 4.5. Утвержденный Список вывешивается на основной входной двери Помещения.
- 4.6. Сотрудники, имеющие право самостоятельной работы в Помещениях:
  - обеспечиваются администратором информационной безопасности под роспись персональными номерными металлическими печатями;
  - узнают от руководителя или от Администратора ИБ ИСПДн коды доступа в Помещение или, в отдельных случаях (при отсутствии в Списке руководителя и/или Администратора ИБ ИСПДн) подготавливают самостоятельно и передают по смене устно.

## 5. РЕЖИМ ДОСТУПА В ПОМЕЩЕНИЯ

- 5.1. Сотрудники, фамилии которых, внесены в утвержденные Списки, имеют право самостоятельно вскрывать (снимать с охраны) и закрывать (сдавать под охрану) Помещения.
- 5.2. Лица, не внесенные в Списки:
  - являются посторонними и могут находиться в Помещении только при наличии тех, кто такое право имеет (в Списки внесен);
  - обязаны покинуть Помещение при отсутствии в нем сотрудников, которые имеют право самостоятельно находиться в Помещении;
- 5.3. В течение рабочего дня сотрудники, внесенные в утвержденные Списки:
  - при оставлении последним Помещения - закрывают дверь Помещения («на замок», «на защелку», в зависимости от технического исполнения запорного устройства);
  - не покидают последними Помещение, если в нем находятся лица, не внесенные в Списки;
  - при обнаружении фактов нарушения режима доступа ставят в известность Администратора ИБ ИСПДн;
  - при посещении Помещения посторонними лицами с целями проведения контрольных, проверочных мероприятий, а также работ по обслуживанию помещений и их инженерно-технических средств ставят в известность об этом Администратор ИБ ИСПДн и начальника Финансового управления.

- 5.4. При обнаружении нарушений режима доступа в Помещения выполняется порядок действий предусмотренный «Инструкцией по действиям персонала в нештатных ситуациях».

## **6. РЕЖИМ ПРИ ОБСЛУЖИВАНИИ И РЕМОНТЕ В ПОМЕЩЕНИИ**

- 6.1. Обслуживание Помещения (уборка или различный ремонт Помещения, инженерно-технического оборудования) проводится обслуживающим персоналом только в присутствии и под присмотром хотя бы одного из сотрудников имеющего право самостоятельно находиться в Помещении.
- 6.2. Механические или электронные ключи от замков дверей Помещений обслуживающему персоналу и/или другим лицам, не допущенных самостоятельно находиться в Помещении, без согласования с ответственным за защиту ПДн, не выдаются.
- 6.3. Сотрудники подразделения, обеспечивающие контроль действий обслуживающего персонала в Помещении, обязаны не допускать несанкционированных действий в отношении компонент ИСПДн, бумажных и магнитных носителей информации, компонент инженерных систем и т.п.
- 6.4. Капитальный и/или иной ремонт, продолжительный по времени и требующий высвобождения рабочей площади Помещения, может проводиться и без присмотра, однако при этом в обязательном порядке:
- компоненты ИСПДн, носители информации должны быть вынесены из ремонтируемого Помещения в другое контролируемое Помещение;
  - по окончанию ремонта должны быть сменены ключи и коды доступа в Помещение (организовывает и контролирует исполнение Администратор ИБ ИСПДн).

## **7. СМЕНА КОДОВ И КЛЮЧЕЙ**

- 7.1. При утере основного или запасного комплекта ключей доступа начальник Финансового управления инициирует служебное расследование, по результатам которого принимается решение или об изготовлении дополнительного комплекта или о смене секрета замка и, соответственно, замене всех комплектов ключей на новые.
- 7.2. Смена кодов доступа и секретов замков в Помещениях организуется руководителем подразделения (как правило, силами Администратора ИБ ИСПДн) в следующих случаях:
- увольнения или перемещения из состава подразделения сотрудника, знавшего код доступа в Помещение или имеющего доступ к ключам доступа;
  - преднамеренного или непреднамеренного разглашения кода доступа в Помещения тем лицам, у которых нет производственной необходимости его знать;

- установленного факта бесконтрольного нахождения в Помещении лиц, у которых нет производственной необходимости знать код доступа или иметь ключи доступа;
  - истечения одного календарного года с момента первичного ввода или последней смены значения кода доступа.
- 7.3. Смена секретов механических замков и/или кодов доступа электромеханических производится с оформлением акта, который доводится под роспись до всех сотрудников, имеющих право самостоятельно находиться в данном Помещении. Коды доступа доводятся до сотрудников администратором информационной безопасности, как правило, устно, с практической демонстрацией правильности работы устройств разграничения и/или контроля доступа. При необходимости записать код доступа на бумаге, последняя оформляется как парольная карта.

## **8. ПОРЯДОК ПЕРЕСМОТРА РЕГЛАМЕНТА**

- 8.1. Регламент подлежит полному пересмотру в случае приобретения новых технических средств разграничения и контроля доступа. В остальных случаях осуществляется частичный пересмотр настоящего Регламента.
- 8.2. Полный пересмотр данного Регламента проводится с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в Организации.
- 8.3. Частичный пересмотр данного документа проводится ответственным за защиту ПДн.
- 8.4. Внесение изменений в обязательном порядке фиксируется в «Листе регистрации изменений в Регламенте». Лист регистрации изменений в Регламенте представлен в Приложении 2.
- 8.5. Вносимые изменения не должны противоречить другим положениям Регламента.

## **9. ОТВЕТСТВЕННЫЕ ЗА ВЫПОЛНЕНИЕ РЕГЛАМЕНТА**

- 9.1. Ответственность за организацию контрольных и проверочных мероприятий по вопросам доступа в Помещения возлагается на ответственного за защиту ПДн.
- 9.2. Ответственность за своевременное доведение Регламента до сотрудников в части их компетенции и обеспечение условий для выполнения требований данного Регламента возлагается на руководителей подразделений.
- 9.3. Ответственность за соблюдение требований настоящего Регламента возлагается на Администратора ИБ ИСПДн и сотрудников Учреждения.
- 9.4. Администратор ИБ ИСПДн проводит текущий контроль выполнения сотрудниками подразделений требований Регламента.





## ПРИЛОЖЕНИЕ 1 ФОРМА СПИСКА СОТРУДНИКОВ

Утверждаю

Директор МБОУ СОШ №26

\_\_\_\_\_ Н.А.Шишкин

«\_\_» \_\_\_\_\_ 2018 г.

СПИСОК  
СОТРУДНИКОВ, ИМЕЮЩИХ ПРАВО САМОСТОЯТЕЛЬНО НАХОДИТЬСЯ В  
ПОМЕЩЕНИИ № \_\_\_\_\_

№ п/п	Ф.И.О.	должность	№ личной металлической печати

Администратор информационной  
безопасности\_\_\_\_\_ Ф.И.О.  
дата, роспись

Ознакомлены сотрудники

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## ПРИЛОЖЕНИЕ 2 ФОРМА РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РЕГЛАМЕНТЕ

ЛИСТ № \_\_\_\_\_ регистрации изменений в Регламенте

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

**ПРИЛОЖЕНИЕ 3  
ПЕРЕЧЕНЬ ПОМЕЩЕНИЙ С ИСПДН**

Перечень помещений, предназначенных для размещения информационных систем персональных данных  
в МБОУ СОШ №26 г.Ставрополя

№ п/п	Наименование помещения	Наименование подразделения, расположенного в помещении	Ответственный за помещение (ФИО, должность)	Наименование ИСПДн, размещенных в помещении	Примечание

