



**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 497
НЕВСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА**

193079 г. Санкт-Петербург, Октябрьская набережная, дом 70, корпус 2, литер А,
тел./факс 8-812-446-77-58 официальный сайт: <http://школа497.рф>
электронная почта: info.sch497@obr.gov.spb.ru

РАССМОТРЕНО И ПРИНЯТО
Педагогическим советом

Протокол от 29.08.25 № 1

УТВЕРЖДАЮ

Директор

О.А. Коноплева

Приказ от 29.08.25 № 138/2



**ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩИХСЯ,
РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) И РАБОТНИКОВ В
ГБОУ ШКОЛЕ №497 НЕВСКОГО РАЙОНА САНКТ_ПЕТЕРБУРГА**

Санкт-Петербург
2025

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение регламентирует порядок обеспечения защиты персональных данных (ПДн) в ГБОУ школа № 497 (далее — школа) при их обработке в информационных системах и бумажных носителях.

1.2. Положение обязательно для исполнения всеми работниками школы, имеющими доступ к ПДн.

2. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПДН

2.1. Ответственность за организацию защиты ПДн возлагается на директора школы.

2.2. Непосредственное руководство осуществляет заместитель директора, назначенный приказом директора ответственным за обработку и защиту ПДн.

2.3. В школе создаётся рабочая группа по внедрению мер защиты ПДн в составе:

- Заместитель директора по ИКТ;
- Учитель информатики;
- Системный администратор;
- Представитель администрации.

3. РЕЖИМ ДОСТУПА К ПДН

3.1. Доступ к ПДн предоставляется только на основании служебной необходимости.

3.2. Уровни доступа:

Роль	Доступные данные	Ограничения
Классный руководитель	ПДн обучающихся своего класса	Только в рамках учебной деятельности
Учитель-предметник	ФИО, успеваемость по предмету	Без медицинских и семейных данных
Администрация	Полные ПДн в рамках компетенции	С обязательной авторизацией
Технический персонал	Только технические метаданные	Без доступа к содержанию ПДн

3.3. Запрещено:

- Использовать общие учётные записи;
- Передавать логины и пароли третьим лицам;
- Хранить ПДн на личных устройствах и съёмных носителях без шифрования.

4. ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ

4.1. В школе внедряются следующие меры:

- Обязательная авторизация пользователей в информационных системах;
- Регулярное обновление паролей (не реже 1 раза в 3 месяца);
- Установка и обновление антивирусного ПО на всех АРМ;
- Контент-фильтрация интернет-трафика;
- Резервное копирование критичных данных не реже 1 раза в неделю.

4.2. При использовании внешних информационных систем обеспечивается:

- Передача данных только по защищённым каналам (HTTPS);
- Минимизация объёма передаваемых ПДн;
- Контроль за отзывом доступа при завершении работы.

5. ИНСТРУКТАЖ И КОНТРОЛЬ

5.1. Все работники школы, работающие с ПДн, проходят вводный и периодический инструктаж по защите информации (не реже 1 раза в год).

5.2. Факт прохождения инструктажа фиксируется в Журнале учёта инструктажей по информационной безопасности.

5.3. Контроль за соблюдением Положения осуществляет заместитель директора по ИБ. Нарушения рассматриваются в порядке дисциплинарной ответственности.

6. ДЕЙСТВИЯ ПРИ ИНЦИДЕНТАХ

6.1. При выявлении утечки ПДн или несанкционированного доступа работник обязан немедленно сообщить заместителю директора по ИБ.

6.2. В течение 24 часов составляется Акт об инциденте с указанием:

- Даты, времени и обстоятельств инцидента;
- Категории и объёма затронутых ПДн;
- Принятых мер по локализации последствий.

6.3. При необходимости школа уведомляет Роскомнадзор и субъектов ПДн в порядке, установленном законодательством.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Положение вступает в силу с даты утверждения и действует бессрочно.

7.2. Изменения в Положение вносятся приказом директора школы.

Разработал:

Заместитель директора М.А. Дугин _____ /подпись/

