

УЧТЕНО:

Мнение профсоюзного
комитета ГБДОУ
детского сада № 43
Протокол №28
от «23» июня 2022 г.



ПРИНЯТО:

Общее собрание работников
образовательного учреждения
Протокол №8
от «23» июня 2022 г.

УТВЕРЖДАЮ:

Заведующий ГБДОУ
детского сада № 43
Ж. П. Курочкина
Присвоено 23.06.2022
№ 104



ПОРЯДОК

**доступа работников Государственного бюджетного дошкольного
образовательного учреждения детский сад №43
Приморского района Санкт-Петербурга в помещения,
в которых ведется обработка информации ограниченного доступа,
и расположены средства криптографической защиты информации**

1. Общие положения

1.1. Настоящий Порядок доступа работников в помещения Государственного бюджетного дошкольного образовательного учреждения детский сад №43 Приморского района Санкт-Петербурга (далее – ГБДОУ), в которых ведется обработка информации ограниченного доступа, в том числе персональных данных, (далее - Информация) не содержащей сведения, составляющие государственную тайну, и расположены средства криптографической защиты информации разработан в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных», приказом Федерального агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» и другими нормативными правовыми актами.

1.2. Обеспечение безопасности Информации от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении Информации достигается, в том числе, установлением правил доступа в помещения, где обрабатывается Информация с использованием и/или без использования средств автоматизации.

1.3. Размещение информационных систем (далее - ИС), в которых обрабатывается Информация, должно осуществляться в пределах контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации. Для помещений, в которых обрабатывается Информация (далее - Помещения) и расположены средства криптографической защиты информации (далее - СКЗИ), организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей Информации и средств защиты информации, криптосредств и ключевых документов к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц и просмотра ведущихся там работ.

2. Допуск в помещения, в которых ведётся обработка информации ограниченного доступа

2.1. В помещения, где размещены технические средства, позволяющие осуществлять обработку Информации, а также хранятся носители Информации, допускаются только работники, уполномоченные на обработку Информации (в соответствии с Перечнем лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах), а также только лица, имеющие право доступа в помещения ГБДОУ, где осуществляется обработка Информации (в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой и парольной информации СКЗИ информационных систем ГБДОУ).

2.2. При оборудовании Помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

2.3. Нахождение в помещениях с ИС лиц, не включенных в перечни, настоящего порядка, возможно только в присутствии работника, уполномоченного на обработку Информации в данном помещении. Время нахождения в помещениях ограничивается временем решения вопросов, в рамках которого возникла необходимость пребывания в помещении.

2.4. Работники, допущенные к обработке Информации, не должны покидать Помещение, не убедившись, что доступ посторонних лиц к Информации невозможен. Запрещается оставлять материальные носители Информации без присмотра в незапертом помещении.

2.5. Помещения, в которых ведется обработка Информации и расположены средства криптографической информации, должны быть оснащены входными дверьми с замками. Кроме того, должно быть обеспечено постоянное закрытие дверей таких помещений на замок и их открытие только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

2.6. После окончания рабочего дня дверь каждого помещения, в котором ведется обработка Информации, закрывается на ключ.

2.7. В нерабочее время помещения, в которых осуществляется функционирование СКЗИ, все окна и двери должны быть надежно закрыты, ключевые документы убраны в запираемые шкафы (сейфы).

2.8. Ключ выдается сотрудником, ответственным за ведение журнала учёта ключей от помещений.

3. Допуск лиц в помещения

3.1. Для предотвращения просмотра извне окна Помещений должны быть защищены шторами или жалюзи.

3.2. Окна Помещений, расположенных на первых этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, оборудуются металлическими решетками, или другими средствами, препятствующими неконтролируемому проникновению в Помещения.

3.3. При утрате ключа от входной двери в помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей. Факт изготовления новых ключей должен быть документально оформлен в виде акта в произвольной форме.

3.4. Внутренний контроль за соблюдением порядка доступа в помещения, проводится в порядке, определенном в плане проведения внутреннего контроля соответствия требованиям по защите. Контроль и управление физическим доступом к информационным системам и средствам криптографической защиты должны предусматривать:

- поддержание в актуальном состоянии Перечня лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах и Перечня лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой и парольной информации СКЗИ информационных систем ГБДОУ;

- санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены - выдача ключей от помещений строго в соответствии с утвержденным перечнем лиц;

- учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены - выдача ключей от помещений под подпись в соответствующем журнале.

3.5. В обычных условиях помещения и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями СКЗИ или ответственным пользователем СКЗИ.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ. Прибывший ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации информации ограниченного доступа и к замене скомпрометированных криптоключей.

3.6. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка Информации и расположены средства криптографической информации, возлагается на сотрудников, уполномоченных на обработку Информации в ГБДОУ.

3.7. В случае нарушения настоящего Порядка работники могут быть привлечены к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации.

УЧТЕНО:

Мнение профсоюзного
комитета ГБДОУ
детского сада № 43
Протокол №28
от «23» июня 2022 г.



ПРИНЯТО:

Общее собрание работников
образовательного учреждения
Протокол №8
от «23» июня 2022 г.

УТВЕРЖДАЮ:

Заведующий ГБДОУ
детского сада № 43
Ж.К. Курочкина
Приказ от 23.06.2022
№ 19-д



ПОЛОЖЕНИЕ
об использовании простой электронной подписи
в Государственном бюджетном дошкольном образовательном
учреждении детский сад № 43 компенсирующего вида
Приморского района Санкт-Петербурга

1. Общие положения

1.1. Данное Положение об использовании простой электронной подписи в Государственном бюджетном дошкольном образовательном учреждении детский сад № 43 компенсирующего вида Приморского района Санкт-Петербурга (далее – ГБДОУ) разработано в соответствии с Федеральным законом № 273-ФЗ от 29.12.2012 года «Об образовании в Российской Федерации» с изменениями на 30 декабря 2021 года, Федеральным законом №63-ФЗ от 06.04.2011 года «Об электронной подписи» с изменениями на 30 декабря 2021 года, приказом Министерства связи массовых коммуникаций Российской Федерации №107 от 13 апреля 2012 года «Об утверждении Положения о федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" с изменениями на 7 июля 2016 года, а также Уставом ГБДОУ и другими нормативными правовыми актами Российской Федерации, регламентирующими деятельность организаций, осуществляющих образовательную деятельность.

1.2. Настоящее Положение об использовании простой электронной подписи в ГБДОУ (далее – Положение) определяет основные термины, регулирует правила и средства использования простых электронных подписей и регламентирует создание сертификата ключа проверки электронных подписей, устанавливает порядок и условия работы сотрудников с электронными документами в информационной системе (далее – ИС), а также права, обязанности и ответственность владельца простой электронной подписи.

1.3. Единая система идентификации и аутентификации является информационным элементом инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.

1.4. Педагогические работники ГБДОУ, являясь участниками электронного взаимодействия на условиях настоящего Положения, подписывают Уведомление об ознакомлении с Положением (см. *Приложение 1*). Подписание сотрудником ГБДОУ Уведомления равнозначно присоединению к соглашению об участии во внутреннем электронном документообороте с использованием простой электронной подписи на условиях настоящего Положения в соответствии со ст. 428 Гражданского кодекса Российской Федерации («Договор присоединения»).

1.5. Реализация условий применения простой электронной подписи обеспечивает придание юридической силы внутренним электронным документам образовательной организации в ИС, требующим личной подписи Заведующего ГБДОУ, и операциям с ними.

1.6. Наличие простой электронной подписи в электронном документе подтверждает авторство данного документа и сохраняет его целостность. Таким образом, документ, содержащий простую электронную подпись, не может быть изменен после подписания.

1.7. Для подписания документов в ИС используется простая электронная подпись в виде присоединяемой к документу информации, генерируемой программой или информационной системой совместно с пользователем или по его команде.

1.8. В качестве публичной части ключа простой электронной подписи в ГБДОУ используется уникальное имя учетной записи, применяемое для авторизации пользователя в ИС. В качестве конфиденциальной части ключа простой электронной подписи в ГБДОУ используется пароль к учетной записи.

1.9. Изготовление (генерацию), выдачу и регистрацию в ИС имен пользователей и паролей осуществляет назначенное по приказу заведующего ГБДОУ ответственное лицо (далее – Ответственный за техническую поддержку ИС).

1.10. Пароль пользователя ИС может быть изменен его владельцем в любой момент после авторизации в информационной системе. Рекомендуется изменять пароль не реже одного раза в три месяца. Для снижения риска подбора пароля и несанкционированного использования другим лицом ключа электронной подписи рекомендуется не задавать пароли, использованные ранее.

1.11. Создание и выдачу сертификатов ключей проверки электронных подписей осуществляет Удостоверяющий центр на основании соглашения между удостоверяющим центром и образовательной организацией.

2. Основные термины и их определения

2.1. **Электронная подпись** — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2.2. **Сертификат ключа проверки электронной подписи** — электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

2.3. **Владелец сертификата ключа проверки электронной подписи** — лицо, которому в установленном соответствующим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.

2.4. **Ключ электронной подписи** — уникальная последовательность символов, предназначенная для создания электронной подписи.

2.5. **Ключ проверки электронной подписи** — уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

2.6. **Участники электронного взаимодействия** — осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане.

2.7. **Информационная система общего пользования** — информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

2.8. **Удостоверяющий центр** — юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом №63-ФЗ «Об электронной подписи».

3. Электронная подпись и её виды

3.1. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

3.2. К видам электронных подписей относятся:

- простая электронная подпись;
- усиленная электронная подпись.

Различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

4. Правила и средства использования простых электронных подписей

4.1. Электронный документ считается подписанным простой электронной подписью при выполнении следующих условий:

- простая электронная подпись содержится в самом электронном документе;
- ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором ИС, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном

документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

4.2. Нормативные правовые акты и (или) соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать, в частности:

- правила определения лица, подписывающего электронный документ, по его простой электронной подписи;
- обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность.

4.3. Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые:

- позволяют установить факт изменения подписанного электронного документа после момента его подписания;
- обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки;
- позволяют создать электронную подпись в формате, устанавливаемом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, и обеспечивающем возможность ее проверки всеми средствами электронной подписи.

4.4. При создании электронной подписи средства электронной подписи должны:

- показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание электронной подписи, содержание информации, подписание которой производится;
- создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;
- однозначно показывать, что электронная подпись создана.

4.5. При проверке электронной подписи средства электронной подписи должны:

- показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписанной с использованием указанных средств, содержание электронного документа, подписанного электронной подписью, включая визуализацию данной электронной подписи, содержащую информацию о том, что такой документ подписан электронной подписью, а также о номере, владельце и периоде действия сертификата ключа проверки электронной подписи;
- показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;
- указывать на лицо, с использованием ключа электронной подписи, которого подписаны электронные документы.

5. Сертификат ключа проверки электронной подписи

5.1. Удостоверяющий центр:

- создаёт сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата;
- осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи,

соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;

- устанавливает сроки действия сертификатов ключей проверки электронных подписей;

- аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;

- выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

- ведет реестр выданных и аннулированных сертификатов ключей проверки электронных подписей;

осуществляет проверку электронных подписей по обращениям участников электронного взаимодействия.

5.2. Сертификат ключа проверки электронной подписи содержит следующую информацию:

- уникальный номер сертификата ключа проверки электронной подписи, даты начала и окончания срока действия такого сертификата;

- фамилия, имя и отчество заявителя или информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;

- уникальный ключ проверки электронной подписи;

- наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;

- наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи.

5.3. Сертификат ключа проверки электронной подписи прекращает свое действие:

- в связи с истечением установленного срока его действия;

на основании заявления владельца сертификата ключа проверки электронной подписи;

- в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам.

6. Обеспечение юридической силы внутренних электронных документов

6.1. Период работы над электронными документами включает создание и другие действия по их обработке, отражение в учёте, а также публикация на сайте общеобразовательной организации.

6.2. Простая электронная подпись является равнозначной собственноручной подписи на бумажном носителе.

6.3. Полномочия владельца простой электронной подписи, подписавшего электронный документ, подтверждаются в момент подписания в ИС автоматически по положительному результату следующих проверок:

- соответствующий пользователь авторизован в информационной системе;

- соответствующая уникальная последовательность символов электронной подписи включена в реестр выданных электронных подписей;

- соответствующая уникальная последовательность символов электронной подписи отсутствует в реестре отозванных электронных подписей.

6.4. Время формирования электронной подписи фиксируется в момент подписания по московскому времени (UTC+3).

6.5. Визуализация штампа простой электронной подписи на электронном документе, выполненная средствами ИС, является подтверждением факта подписания данного документа соответствующим владельцем электронной подписи.

6.6. Хранение документов осуществляется путем их записи в хранилище электронных документов, которое является частью ИС до окончания срока действия документов.

6.7. Копия электронного документа может быть распечатана на бумажном носителе средствами информационной системы и заверена в установленном порядке.

7. Права, обязанности и ответственность владельца простой электронной подписи

7.1. Владелец простой электронной подписи имеет право:

- вести электронные документы, подписанные электронной подписью при размещении их на сайте образовательной организации, согласно приказу №831 Федеральной службы по надзору в сфере образования и науки «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети "Интернет" и формату представления информации», которые должны соответствовать условиям ст.6 №63-ФЗ «Об электронной подписи» для их признания равнозначными документам на бумажном носителе, подписанным собственноручной подписью;

- обращаться к заведующему ГБДОУ для разбора конфликтных ситуаций (споров), возникающих при применении простой электронной подписи.

7.2. Владелец простой электронной подписи обязан:

- осуществлять обработку внутренних электронных документов в соответствии со своими должностными обязанностями;

- учитывать и принимать все возможные меры для предотвращения несанкционированного использования своего ключа электронной подписи;

- ни при каких условиях не передавать ключ электронной подписи другим лицам;

- при компрометации своего ключа электронной подписи незамедлительно обратиться к ответственному за техническую поддержку ИС для приостановки действия принадлежащего ему ключа электронной подписи;

- соблюдать конфиденциальность ключа простой электронной подписи.

7.3. Владелец простой электронной подписи несет личную ответственность за сохранность своего ключа электронной подписи и его защиту от несанкционированного использования.

8. Заключительные положения

8.1. Настоящее Положение об использовании простой электронной подписи в ГБДОУ является локальным нормативным актом, принимается на Общем собрании ГБДОУ после согласования с Профсоюзным комитетом ГБДОУ и утверждается (либо вводится в действие) приказом заведующего учреждения, осуществляющего образовательную деятельность.

8.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.

8.3. Данное Положение принимается на неопределенный срок. Изменения и дополнения к Положению принимаются в порядке, предусмотренном п.8.1. настоящего Положения.

8.4. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

Приложение № 1
к Положению об использовании простой
электронной подписи в ГБДОУ
детский сад № 43 Приморского района
Санкт-Петербурга

ПЕРЕЧЕНЬ ДОКУМЕНТОВ

Участники внутреннего электронного документооборота в ГБДОУ детский сад №43 Приморского района Санкт-Петербурга используют простую электронную подпись при обработке следующих электронных документов:

- локальные нормативные акты (приказы, положения, инструкции, регламенты),
- образовательные программы,
- рабочие программы,
- исходящие письма,
- отчеты, графики, расписания

Приложение № 2
к Положению об использовании простой
электронной подписи в ГБДОУ
детский сад № 43 Приморского района
Санкт-Петербурга

**Уведомление об ознакомлении
с Положением об использовании простой
электронной подписи в Государственном бюджетном дошкольном
образовательном учреждении детский сад № 43 компенсирующего вида
Приморского района Санкт-Петербурга**

Я, _____
(ФИО, должность)

именуемый в дальнейшем «Работник», настоящим подтверждаю, что ознакомился с Положением об использовании простой электронной подписи в Государственном бюджетном дошкольном образовательном учреждении детский сад № 43 компенсирующего вида Приморского района Санкт-Петербурга, а именно: Работник признает равнозначность своей простой электронной подписи собственноручной подписи на бумажном носителе и заявляет о присоединении к соглашению об участии во внутреннем электронном документообороте с использованием простой электронной подписи на условиях Положения об использовании простой электронной подписи в образовательной организации в соответствии со ст. 428 Гражданского кодекса РФ («Договор присоединения») с «_____» _____ 202__ года.

«_____» _____ 202__ г.

(Подпись)

(Расшифровка подписи)