УЧТЕНО:	ПРИНЯТО:	УТВЕРЖДАЮ:
Мнение профсоюзного комитета ГБДОУ детского сада № 43 Протокол №28 от «23» июня 2022 г.	Общее собрание работников образовательного учреждения Протокол №8 от «23» июня 2022 г.	Заведующий ГБДОУ детского сада № 43 _____ Л.Н. Курочкина Приказ от 23.06.2022 № 69-1

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

Санкт-Петербург
2022

1. Общие положения

1.1. Настоящий Порядок доступа работников в помещения Государственного бюджетного дошкольного образовательного учреждения детский сад №43 Приморского районаСанкт-Петербурга (далее – ГБДОУ), в которых ведется обработка информации ограниченного доступа, в том числе персональных данных, (далее - Информации) 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:

- поддерживание 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.