



Совет депутатов Вачского муниципального округа Нижегородской области

РАСПОРЯЖЕНИЕ

от 27.01.2023 г.

№ 20-х

О доступе работников в помещения,
в которых ведется обработка информации
ограниченного доступа и расположены средства
криптографической защиты информации

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», приказом Федерального агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 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», приказом Федеральной службы безопасности России от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» и в целях организации доступа работников Совета депутатов Вачского муниципального округа Нижегородской области в помещения, в которых ведется обработка информации ограниченного доступа и расположены средства криптографической защиты информации (далее – СКЗИ):

1. Утвердить порядок доступа работников в помещения, в которых ведется обработка информации ограниченного доступа, и расположены СКЗИ согласно приложению 1 к настоящему распоряжению;

2. Утвердить перечень лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой и парольной информации согласно приложению 2 к настоящему распоряжению;

3. Контроль за исполнением настоящего распоряжения оставляю за собой.

Председатель Совета депутатов

С.Е Липов

**Порядок
доступа работников в помещения, в которых ведется обработка
информации ограниченного доступа, и расположены средства
криптографической защиты информации**

1. Общие положения

Настоящий порядок доступа работников Совета депутатов Вачского муниципального округа Нижегородской области (далее – Совет депутатов) в помещения администрации Вачского муниципального округа Нижегородской области (далее – администрация), 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 № 152-ФЗ «О персональных данных», приказом Федерального агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 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», приказом Федеральной службы безопасности России от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

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.

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, крипто средств 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**

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 приказом об утверждении перечня должностей, допущенных к обработке персональных данных), а также только лица, имеющие право доступа в помещения Совета депутатов, администрации, 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).

При оборудовании помещений должны выполняться требования к размещению, монтажу крипто средств, а также другого оборудования, функционирующего с крипто средствами.

Для каждого помещения, в котором обрабатываются персональные данные, (далее – ЗП), должен быть назначен соответствующий ответственный за режим безопасности и правильность использования установленных в нем технических средств.

Перечень ЗП Совета депутатов и ответственных за режим безопасности в них утверждает председатель Совета депутатов.

Нахождение в помещениях с ИС лиц, не включенных в перечни доступа 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.

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.

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.

Помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

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

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

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

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

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

При утрате ключа от хранилища или 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. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

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;

- 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 помещения 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.

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.

Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка Информации и расположены средства криптографической информации, возлагается на сотрудника, уполномоченного на обработку Информации в Совете депутатов.

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

Приложение 2
к распоряжению Совета депутатов
Вачского муниципального округа
Нижегородской области
от 27.01.2023 года № 20-х

ПЕРЕЧЕНЬ

лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой и парольной информации

Наименование должности	Ф.И.О. муниципального служащего	Место хранения
Председатель Совета депутатов	Липов Сергей Евгеньевич	кабинет №34,32,21,18
Начальник отдела Совета депутатов	Антонова Наталья Владимировна	кабинет № 34,32,21,18